Issues in Homeland Security Policy for the 112th Congress

William L. Painter, Coordinator
Analyst in Emergency Management and Homeland Security Policy

September 22, 2011

Congressional Research Service
7-5700
www.crs.gov
R42025

CRS Report for Congress
Prepared for Members and Committees of Congress

Summary

With the tenth anniversary of the September 11th terrorist attacks, many observers are making a fresh assessment of where America's homeland security enterprise stands today. In the wake of those attacks, Congress made extensive changes to the structure and function of many agencies, establishing a consolidated Department of Homeland Security and dedicating significant additional resources expressly to the security of the homeland. After the initial surge of activity, evolution of America's response has continued under the leadership of different Administrations, Congresses, and in a shifting environment of public opinion.

This report outlines an array of homeland security issues that may come before the 112th Congress. After a brief discussion of the overall homeland security budget, the report divides the specific issues into five rough categories:

- Counterterrorism and Security Management
- Border Security and Trade
- Immigration
- Disaster Preparedness, Response, and Recovery
- Departmental Management

In each of those areas, you will find a survey of topics briefly analyzed by Congressional Research Service experts. The information included only scratches the surface on most of these issues. For more detailed information, you may choose to consult their more in-depth works or consult directly with the individual authors.

This report will not be updated.

Contents

Contacts

What Is Homeland Security?

This question has dogged U.S. public policy debates for ten years. At this point, there is no statutory definition of homeland security. What conventional wisdom defines as "homeland security missions" and the missions undertaken by the Department of Homeland Security are not the same.

The Department of Homeland Security (DHS) was established by the Homeland Security Act of 2002 (P.L. 107-296), which was signed into law on November 25, 2002. The new department was assembled from components pulled from 22 different government agencies and began official operations on March 1, 2003. Since then, DHS has undergone a series of restructurings and reorganizations to improve its effectiveness and efficiency.

Although at this point, DHS does include many of the homeland security functions of the federal government, many of these functions or parts of these functions remain at their original executive branch agencies and departments, including the Departments of Justice, State, Defense, and Transportation. Not all of the missions of the Department are officially "homeland security" missions, either. Some components have historical missions that do not directly relate to conventional homeland security definitions, such as the Coast Guard's environmental and boater safety missions, and Congress has debated whether FEMA and its disaster relief and recovery missions belong as a part of the Department.

Some issues have implications for homeland security, such as the role of the military in law enforcement, monitoring and policing transfers of money, human trafficking, explosives and weapons laws, and several aspects of foreign policy, trade, and economics.

Rather than trying to resolve this debate, this report is limited to topics that generally fall within the four mission study areas used to develop the Quadrennial Homeland Security Review mandated by the Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L. 110-53):

- Counterterrorism and Security Management
- Border Security and Trade
- Immigration
- Disaster Preparedness, Response, and Recovery

A fifth section covering management issues at DHS rounds out the discussion.

The issues included in this report do not represent a comprehensive list of possible issues—they represent a broad array of issues likely to be addressed by Congress in the coming months.

The Budget and Security

According to a recent analysis of data from the Office of Management and Budget (OMB) conducted by the National Priorities Project, the U.S. government has spent $636 billion (adjusted for inflation) on homeland security in the wake of the 9/11 attacks. According to the Project's

analysis, spending on homeland security activities has risen over 300% from 2001 to 2011.[1] Funding rose every year until it peaked in FY2009 at $74 billion. The total budget request for homeland security activities for FY2012 is $71.6 billion, a reduction of nearly $2.4 billion from its high-water mark in nominal terms.

In 2010, for the first time since the establishment of the Department of Homeland Security, neither the House nor the Senate completed work on its version of an appropriations bill for the department. This stands in contrast to previous years, when the bill moved relatively easily through the legislative process, despite the emergence of occasional controversial issues. The concurrent resolution provided $41.7 billion in discretionary appropriations for DHS for FY2011, establishing funding levels for some components and activities, while leaving others to be funded at FY2010 levels. The resolution overall gave the department much less explicit direction from Congress than previous funding vehicles, in several cases leaving decisions usually made by Congress about how to allocate limited funds in DHS's hands.[2]

Given the increasing level of concern about the size of the federal government's budget deficit, security spending will continue to be a target for those seeking budget savings. Under the Budget Control and Deficit Reduction Act of 2011, security spending is a newly defined category, including discretionary spending for: the Departments of Homeland Security, Defense, and Veterans Affairs; the National Nuclear Security Administration; the intelligence community management account; and all accounts in the international affairs budget function.[3] These accounts will be limited to $684 billion in FY2012—roughly the level they were funded at in FY2010, and then be required to limit their growth to $2 billion (less than 0.3%) in FY2013.

The current budget environment will likely present challenges to the department going forward, as DHS's ongoing efforts to consolidate its headquarters, recapitalize the Coast Guard, upgrade the department's technology and management systems, complete data center consolidation, and maintain its staffing levels will compete with the budget demands of a limited subset of government agencies for more limited funds. The potential impact of the changed budget environment is discussed at various points throughout this report.

Counterterrorism and Security Management

The Transnational Trend of Terrorism[4]

Terrorism remains a transnational threat that entails risks to U.S. global interests emanating from and manifested in both the international and domestic environment. Central to United States efforts to address transnational terrorism are actions taken to detect, deter, and defeat Al Qaeda.

[1] Chris Hellman, *U.S. Security Spending Since 9/11*, National Priorities Project, Northampton, MA, May 26, 2011, http://nationalpriorities.org/en/publications/2011/us-security-spending-since-911.

[2] For a fuller discussion of this issue, see CRS Report R41189, *Homeland Security Department: FY2011 Appropriations*, coordinated by Jennifer E. Lake and William L. Painter.

[3] Even this broader definition of "security spending" does not include homeland security activities in other departments, such as the Department of Transportation, Department of Justice, and the Department of Energy. For a discussion of the total federal spending on homeland security missions, see the appendix to CRS Report R41982, *Homeland Security Department: FY2012 Appropriations*, coordinated by William L. Painter and Jennifer E. Lake.

[4] Prepared by John Rollins, Specialist in Terrorism and National Security, jrollins@crs.loc.gov, 7-5529.

While recognizing that numerous other terrorist groups may wish to harm U.S. global security interests, the June 2011 release of the Administration's National Strategy for Counterterrorism was nonetheless primarily focused on addressing threats from Al Qaeda.[5] In a statement before the United Nations Counterterrorism Committee on July 20, 2001, Daniel Benjamin, the Coordinator of the Office of the Counterterrorism at the State Department, said "rather than trying to combat directly every single terrorist organization regardless of whether they have the intent or capability to ever attack the U.S. or our citizens, President Obama's counterterrorism strategy is (focused on) Al Qaeda and its affiliates and adherents."[6] Understanding the global nature and capabilities of this subset of terrorist groups and individuals is central to formulating sound strategic policy and overseeing its effective implementation.[7]

The past few years have witnessed an increase in terrorist actions by entities claiming some affiliation with or philosophical connection to Al Qaeda. Many of the past year's global terrorist attacks were conducted by individuals or small terrorist cells that received support ranging from resources and training to having minimal connections, if any, with the terrorist groups to which they claim allegiance. Some argue that recent U.S. counterterrorism successes may be reducing the level of terrorist threats to the nation emanating from core Al Qaeda. U.S. officials suggest that the killing of Osama bin Laden in May 2011 coupled with continuous post-9/11 global military and intelligence counterterrorism actions has significantly degraded Al Qaeda's ability to successfully launch a catastrophic terrorist attack against U.S. global interests.[8] Others suggest that Al Qaeda has changed from an organization to a philosophical movement, making it more difficult to detect and defeat. These security experts suggest that Al Qaeda and associated affiliates will remain viable, due in part to the prospective security implications related to the nation's budgetary situation. Noted author on counterterrorism issues, Daveed Gartenstein-Ross, argues that "the U.S. will not be (defeated) by Al Qaeda. But one can see that as the national debt increases, we (will) have to make spending cuts and as Al Qaeda gets stronger in multiple countries simultaneously – Somali, Yemen, Pakistan, maybe Mali – suddenly you're looking at multiple theaters from where catastrophic strikes can be launched."[9] The long-term fiscal implications of United States counterterrorism policies and responses appear to be of concern to John Brennan, the Assistant to the President for Homeland Security and Counterterrorism. In June 2011, Mr. Brennan spoke of Osama bin Laden's often stated objective of pursuing global acts of terrorism against the nation interests with the desire to "bleed [the U.S.] financially by drawing us into long, costly wars that also inflame anti-American sentiment."[10]

The terrorist threat to U.S. global interests will likely remain a critical issue for the Administration and 112th Congress. Over the past few years numerous individuals were arrested in the homeland and abroad for conducting attacks and planning terrorism-related activities

[5] National Strategy for Counterterrorism, released June 29, 2011, available at http://www.whitehouse.gov/.

[6] Remarks by Daniel Benjamin, Coordinator, State Department, Office of the Coordinator for Counterterrorism, Before the United Nations Counterterrorism Committees, July 20, 2011.

[7] For more information on this issue see CRS Report R41070, *Al Qaeda and Affiliates: Historical Perspective, Global Presence, and Implications for U.S. Policy*, coordinated by John Rollins.

[8] Greg Miller, *U.S. Officials believe al-Qaeda on the Brink of Collapse*, The Washington Post, July 28, 2011. http://www.washingtonpost.com/world/national-security/al-qaeda-could-collapse-us-officials-say/2011/07/21/gIQAFu2pbI_story.html.

[9] Spencer Ackerman, *Even Dead, Osama Has a Winning Strategy*, Wired, July 20, 2011. http://www.wired.com/dangerroom/2011/07/even-dead-osama-has-a-winning-strategy-hint-its-muhammad-alis/.

[10] Remarks by the John Brennan, the Assistant to the President for Homeland Security and Counterterrorism, before the Paul H. Nitze School of Advanced International Studies, June 29, 2011.

directed at U.S. national security interests. All of the attacks—successful and unsuccessful—were of a transnational dimension and ranged from a lone shooter who appears to have become radicalized over the Internet to terrorist organizations wishing to use airliners as platforms for destruction to individuals attempting to detonate large quantities of explosives in symbolic areas frequented by large groups of people.

The first session of the 112th Congress undertook efforts, largely through hearings, to better understand the nature of terrorism in various geographic regions and assess the effectiveness of U.S. and partnering nations' counterterrorism efforts. Programs and policies that the 112th Congress reviewed include public diplomacy efforts; imposition of sanctions; terrorism financing rules; the nexus between international crime, narcotics, and terrorism; and the relationship between domestic and international terrorism activities. The second session of the 112th Congress may desire to assess the Obama Administration's counterterrorism-related strategies, policies, and programs to ascertain if additional guidance or legislation is required. These assessments will likely entail considerations of how best to balance perceived risks to U.S. global security interests with concerns about the long-term fiscal challenges facing the nation.

Homegrown Jihadist Terrorism[11]

As part of a much-discussed apparent increase in terrorist activity in the United States, CRS estimates that since May 2009 arrests have been made in more than 30 homegrown jihadist[12] terrorist plots by American citizens or legal permanent residents of the United States. [13] Two of these resulted in attacks—U.S. Army Major Nidal Hasan's alleged assault at Fort Hood in Texas and Abdulhakim Muhammed's shooting at the U.S. Army-Navy Career Center in Little Rock, AR—that produced 14 deaths. By comparison, in more than seven years from the September 11, 2001 terrorist strikes (9/11) through May 2009, there were 21 such plots.[14] Two resulted in attacks, and never more than six occurred in a single year (2006).[15] The apparent spike in such activity after May 2009 suggests that at least some Americans—even if a tiny minority—are susceptible to ideologies supporting a violent form of jihad. Most of the homegrown plots after

[11] Prepared by Jerome P. Bjelopera, Specialist in Organized Crime and Terrorism, jbjelopera@crs.loc.gov, 7-0622. This section of this report does not presume the guilt of indicted individuals in pending federal cases.

[12] For this report, "homegrown" describes terrorist activity or plots perpetrated within the United States or abroad by American citizens, legal permanent residents, or visitors radicalized largely within the United States. "Jihadist" describes radicalized Muslims using Islam as an ideological and/or religious justification for belief in the establishment of a global caliphate—a jurisdiction governed by a Muslim civil and religious leader known as a caliph—via violent means. Jihadists largely adhere to a variant of Salafi Islam—the fundamentalist belief that society should be governed by Islamic law based on the Quran and adhere to the model of the immediate followers and companions of the Prophet Muhammad.

[13] In a December 7, 2010 report, CRS listed 43 plots and attacks by homegrown jihadists that occurred between September 11, 2001, and November 2010. The number has risen since then, as additional plots occurred after November 2010. See CRS Report R41416, *American Jihadist Terrorism: Combating a Complex Threat*, by Jerome P. Bjelopera. Hereinafter: Bjelopera, *American Jihadist*.

[14] For more information on these attacks see Appendix A in Bjelopera, *American Jihadist.*

[15] The two attacks between 9/11 and May 2009 involved Hasan Akbar and Mohammed Reza Taheri-Azar. On March 23, 2003, two days after the U.S. invasion of Iraq, U.S. Army Sergeant Akbar killed two U.S. Army officers and wounded 14 others at U.S. Army Camp Pennsylvania in Kuwait, 25 miles from the Iraq border. On March 3, 2006, Taheri-Azar, a 22-year-old naturalized American citizen from Iran, drove his sport utility vehicle (SUV) into a crowd at The Pit, a popular student gathering spot at the University of North Carolina at Chapel Hill. The SUV struck and injured several people.

May 2009 likely reflect a trend in jihadist terrorist activity away from schemes directed by core members of significant terrorist groups such as Al Qaeda.

The Threat: Four Key Themes

Homegrown violent jihadist activity since 9/11 defies easy categorization. CRS analysis of the terrorist plots and attacks since 9/11 suggests four broad themes:

- **Various Endgames:** Plots have involved individuals interested in a variety of ways to harm U.S. interests. Some individuals focused their efforts on becoming foreign fighters in conflict zones, such as Somalia. Others planned attacks using explosives, incendiary devices, or firearms. Yet others incorporated multiple, unspecific, or unique tactics. Finally, outside of the post-9/11 violent plots, additional individuals intended only to fund or materially support jihadist activities.
- **Little Interest in Martyrdom:** A minority of homegrown jihadists clearly exhibited interest in killing themselves while engaged in violent jihad.
- **Success of Lone Wolves:** Individuals acting alone, so-called "lone wolves," conducted all four successful homegrown attacks since 9/11.
- **Divergent Capabilities:** The operational capabilities of participants diverge greatly. Some evinced terrorist tradecraft such as bomb-making skills. Others appeared to be far less experienced.

Countering the Threat

The Obama administration has recognized the significance of the homegrown jihadist threat in two of its recent strategy documents. In June 2011 it announced its *National Strategy for Counterterrorism.*[16] The strategy focuses on Al Qaeda, its affiliates (groups aligned with it), and its adherents (individuals linked to or inspired by the terrorist group).[17] John Brennan, President Obama's top counterterrorism advisor publicly described the strategy as the first one, "that designates the homeland as a primary area of emphasis in our counterterrorism efforts."[18]

In August 2011, the Obama Administration also released a strategy for combating violent extremism.[19] It revolves around countering the radicalization of all types of potential terrorists. As such, the radicalization of violent jihadists falls under its purview. The strategy's domestic focus includes general philosophical statements about the importance of protecting civil rights, federal

[16] White House, *National Strategy for Counterterrorism,* June 2011, http://www.whitehouse.gov/sites/default/files/counterterrorism_strategy.pdf. Hereafter: *National Strategy.*

[17] Ibid, p. 3.

[18] Mathieu Rabechault, "U.S. Refocuses on Home-Grown Terror Threat," *AFP,* June 29, 2011, http://www.google.com/hostednews/afp/article/ALeqM5hLyJyB7khhqIxWOOlm1mCj7fYsRQ?docId=CNG.3f90005700ea65e0b05509a135c7a3a8.471; Karen DeYoung, "Brennan: Counterterrorism Strategy Focused on al-Qaeda's Threat to Homeland," *Washington Post*, June 29, 2011, http://www.washingtonpost.com/national/national-security/brennan-counterterrorism-strategy-focused-on-al-qaedas-threat-to-homeland/2011/06/29/AGki1LrH_story.html.

[19] White House, *Empowering Local Partners to prevent Violent Extremism in the United States,* August 2011, http://www.whitehouse.gov/sites/default/files/empowering_local_partners.pdf.

cooperation with local leaders in the private and public sectors, and the insistence that the strategy does not center solely around fighting one particular radical ideology.[20] However, the eight-page document lacks details, especially when compared to the approaches of other nations. The unclassified United Kingdom's counter-radicalization strategy, known as "Prevent," details numerous specific programs and is over 100 pages long.[21] One radicalization expert described the U.S. strategy as "very aspirational."[22]

Congress may wish to consider oversight of the Obama Administration's new strategy to combat violent extremism, since it lacks specifics. From a more strictly counterterrorism perspective, critics also note that there is no national estimate of domestic terrorist threats; national domestic intelligence collection plan; nor domestic intelligence collection requirements, priorities, or coordination. Congress may also wish to consider requiring the Director of National Intelligence to examine whether and how to develop a national domestic intelligence framework or plan as part of a unified strategy to combat violent extremism within the United States.

Radicalization

Radicalization and terrorism are terms that are sometimes used interchangeably but do not necessarily mean the same thing. Radicalization has been described as the exposure of individuals to ideological messages and the movement of those individuals from mainstream beliefs to extremist viewpoints.[23] Others say radicalization consists of changes in belief and behavior to justify intergroup violence and personal or group sacrifice to advance specific closely held ideas.[24] The United Kingdom's "Prevent" counter-radicalization strategy defines radicalization as: "the process by which a person comes to support terrorism and forms of extremism leading to terrorism."[25] The Obama Administration's counter-radicalization strategy frames its discussion around "violent extremists" which it defines as "individuals who support or commit ideologically-motivated violence to further political goals."[26]

While "radicalization" and "terrorism" are certainly related, an important distinction between the terms exists as they relate to the threshold of U.S. law enforcement interest and action. This is because Americans have the right under the First Amendment to adopt, express, or disseminate ideas, even hateful and radical ones. But when radicalized individuals mobilize their views, i.e., they move from a radicalized viewpoint to membership in a terrorist group, or to planning, materially supporting, or executing terrorist activity, then the nation's public safety and security interests are activated.

In the post-9/11 environment, the public expects law enforcement to disrupt terrorist plots *before* an attack occurs. This has lead authorities to adopt a preventive policing approach that focuses not just on crime that has occurred, but on the possibility that a crime may be committed in the future. In this context, a major challenge for

[20] Eileen Sullivan, "New White House Strategy to Hit Violent Extremism," *Associated Press,* August 3, 2011, http://www.google.com/hostednews/ap/article/ALeqM5hLU4EFgXfCXmXryTs3Z3UpSRO8CA?docId=a159313d96c14cff94e4b5a87bc53730.

[21] Home Office, *Prevent Strategy,* June 2011, http://www.homeoffice.gov.uk/publications/counter-terrorism/prevent/prevent-strategy/prevent-strategy-review?view=Binary.

[22] Dina Temple-Raston, "White House Unveils Counter-Extremism Plan," *NPR*, August 3, 2011, http://www.npr.org/2011/08/03/138955790/white-house-unveils-counter-extremism-plan. For more on what a counter-radicalization strategy for the U.S. should broadly entail, see Peter Neumann, *Preventing Violent Radicalization in America,* Bipartisan Policy Center (June 2011), http://www.bipartisanpolicy.org/sites/default/files/NSPG.pdf.

[23] Royal Canadian Mounted Police, National Security Criminal Investigations, *Radicalization: A Guide for the Perplexed*, Canada, June 2009, p. 1.

[24] Clark McCauley and Sophia Moskalenko, "Mechanisms of Political Radicalization: Pathways Toward Terrorism," *Terrorism and Political Violence*, vol. 20, no. 3 (July 2008), p. 416.

[25] Home Office, *Prevent Strategy,* June 2011, p. 108, http://www.homeoffice.gov.uk/publications/counter-terrorism/prevent/prevent-strategy/prevent-strategy-review?view=Binary.

[26] *Empowering Local Partners to Prevent Violent Extremism in the United States,* August 2011, p. 1, http://www.whitehouse.gov/sites/default/files/empowering_local_partners.pdf.

federal law enforcement, particularly the Federal Bureau of Investigation (FBI), is gauging how quickly and at what point individuals move from radicalized beliefs to violence so that a terrorist plot can be detected and disrupted. A 2008 revision to the *Attorney General's Guidelines for Domestic Federal Bureau of Investigation Operations* was intended to be helpful in this regard, streamlining FBI investigations and making them more proactive. The revision permits the Bureau to conduct assessments of individuals or groups without factual predication.[27] However, the new guidelines have generated some controversy among civil libertarians. The FBI is further revising the guidelines.[28]

To counter violent jihadist plots, both U.S. and foreign law enforcement agencies have employed two sets of innovative tactics. Using violations of civil laws to arrest and prosecute suspected terrorists and their support networks is known as taking the "Al Capone" approach, in reference to the federal government's successful use of the mobster's violations of tax law to bring him down. Law enforcement has also successfully used "agents provocateurs" – people employed to associate with suspects and incite them to commit acts that they can be arrested for. These tactics have long been used in a wide variety of criminal cases but have particular utility in counterterrorism investigations as they allow suspects to be arrested prior to the commission of a terrorist act rather than after the damage has been done.

Law enforcement agencies also appreciate that the prevention of terrorist attacks requires the cooperation and assistance of the public, particularly American Muslim communities. Currently, numerous U.S. government agencies conduct outreach, engage, and partner with these communities.

Medical Countermeasures to Chemical, Biological, Radiological, and Nuclear Terrorism[29]

Successful deployment of effective medical countermeasures, such as drugs or vaccines, following a chemical, biological, radiological, or nuclear (CBRN) terrorist attack could reduce the effects of an attack. The federal government has created several programs over the last decade to develop, procure, and distribute CBRN medical countermeasures. Despite these efforts, the pharmacuetical industry has developed only a few new countermeasures and many experts question the government's ability to quickly distribute countermeasures following an attack. The 112th Congress is considering reauthorizing some of these programs, as well as further enhancing the federal government's ability to develop, procure, and distribute medical countermeasures.

In 2004, Congress passed the Project BioShield Act (P.L. 108-276) to encourage the private sector to develop CBRN medical countermeasures by creating a guaranteed federal market.[30] Congress

[27] According to the *Guidelines*, Section II, "Investigations and Intelligence Gathering," (p. 17), "Assessments … require an authorized purpose but not any particular factual predication.… [T]he FBI must proactively draw on available sources of information to identify terrorist threats and activities. It cannot be content to wait for leads to come in through the actions of others, but rather must be vigilant in detecting terrorist activities to the full extent permitted by law, with an eye towards early intervention and prevention of acts of terrorism before they occur." For more information see CRS Report R41780, *The Federal Bureau of Investigation and Terrorism Investigations*, by Jerome P. Bjelopera.

[28] Charlie Savage, "F.B.I. Agents Get Leeway to Push Privacy Bounds," *New York Times,* June 12, 2011, http://www.nytimes.com/2011/06/13/us/13fbi.html?_r=2&hp.

[29] Prepared by Frank Gottron, Specialist, Science and Technology Policy, fgottron@crs.loc.gov.

advance appropriated $5.6 billion for Project BioShield acquisitions for FY2004-FY2013. Through July 2011, the federal government had obligated $2.563 billion of this advance appropriation to acquire CBRN countermeasures. Congress removed an additional $1.461 billion from this account through rescission or transfers to other programs. The President has requested transferring $765 million from this account to other CBRN-development related accounts for FY2012. Congress is also considering other Project BioShield related proposals. These include whether to extend the program authority beyond FY2013, whether to change the structure and purpose of the account, and how much funding should be authorized for acquisition through this account.

In 2006, Congress passed the Pandemic and All-Hazard Preparedness Act (P.L. 109-417) creating the position of the Assistant Secretary for Preparedness and Response (ASPR) in the Department of Health and Human Services (HHS), in part, to improve the planning, coordination, and accountability of the government's efforts to perform CBRN countermeasure advanced research, development, and procurement. Congress is considering whether changes to existing programs or new programs would further improve governmentwide CBRN countermeasure efforts. These include moving programs for countermeasure stockpiling and distribution to ASPR, allowing more flexibility in using Project BioShield-appropriated funds, and improving planning and transparency by requiring a new countermeasure implementation plan and a five-year budget plan. Additionally, the President has requested the creation of a nongovernmental strategic investment firm. This firm would provide capital and business advice to small companies developing medical countermeasure-related technologies that could fill government needs.

Distribution of existing medical countermeasures against potential CBRN agents remains a challenge. The federal government has attempted to address this challenge through programs that stockpile and distribute stores of medical countermeasures, including the Centers for Disease Control and Prevention's (CDC's) Strategic National Stockpile (SNS). Many experts question the sufficiency of current federal programs to distribute federal stockpiles to states and localities in the midst of an emergency, and whether state governments have sufficient plans, organization, and resources to receive federal stockpiles and effectively disseminate them. The 112th Congress is considering whether transferring the CDC's SNS to ASPR would improve the efficiency and coordination of the countermeasure development and procurement programs with the stockpiling and distribution programs. Congress is evaluating the effectiveness of current federal programs designed to help state and local governments improve their stockpiling and distribution programs. Congress may also consider to what extent other stockpiling and distribution methods should augment the SNS. Such methods include home or business countermeasure stockpiling and using the postal service to distribute countermeasures. These proposals may improve countermeasure distribution but also raise some issues regarding program costs, unintended use of stockpiles, and ability of local authorities to fully implement programs. Finally, Congress may consider HHS's request for changes to its authority to allow the use of unapproved countermeasures in emergencies. According to HHS, these changes would allow greater flexibility in prepositioning countermeasures and thus improve countermeasure distribution in response to an emergency.

(...continued)

[30] See CRS Report R41033, *Project BioShield: Authorities, Appropriations, Acquisitions, and Issues for Congress*, by Frank Gottron.

Terrorist Screening and Background Checks for Firearms and Explosives[31]

The November 2009 Fort Hood shootings renewed interest in terrorist watch lists and firearms-related background checks through the National Instant Criminal Background Check System (NICS). Since February 2004, when the Department of Justice first incorporated terrorist watch list checks into the NICS process, three possible issues have emerged for Congress. First, should terrorist watch list checks be incorporated statutorily into the firearms- and explosives-related background check processes? Second, should approved firearm transfer records be maintained on a temporary basis to determine whether persons of interest in counterterrorism investigations have obtained firearms improperly? Third, should persons watch-listed as known or suspected terrorists be prohibited statutorily from possessing firearms and explosives?

Before 2004, the Federal Bureau of Investigation (FBI) did not conduct terrorist watch list queries as part of NICS background checks pursuant to the Brady Handgun Violence Prevention Act (P.L. 101-159). Such watch list checks were not conducted, because being a known or suspected terrorist was not, and is not, a disqualifying factor for firearms or explosives transfer and possession eligibility. In February 2004, however, the FBI modified its NICS operating procedures and began querying terrorist watch list records for both firearms and explosives transfers. Terrorist watch list records were downloaded into the National Crime Information Center (NCIC), one of the computer systems that is queried by NICS and includes several "hot files" on persons who are of interest to U.S. law enforcement agencies, and who are also usually prohibited under federal law from possessing a firearm and/or explosives.

Today, the NCIC "hot file" into which terrorist watch list records are downloaded is the Known and Appropriately Suspected Terrorist (KST) file. Formerly, watch list records were downloaded into the NCIC Violent Gang and Terrorist Offender File (VGTOF). Information related to the subjects of NICS-generated terrorist watch list hits were, and are, passed on to FBI Counterterrorism Division and special agents in the field, who are usually members of Joint Terrorism Task Forces (JTTFs) for two purposes, principally: (1) to validate the match between the individual and the watch list record, and (2) to check for information that would prohibit that individual, the prospective transferee, licensee, or permittee, from possessing firearms or explosives (e.g., illegal immigration or fugitive status). Despite these measures, the Government Accountability Office (GAO) has reported that subjects of valid terrorist watch list matches have been transferred firearms and, less frequently, explosives.[32] Beginning in the 109th Congress, these GAO reports lent impetus to legislative proposals that would grant the Attorney General authority to not only screen applicants against the terrorist watch list, but to deny them firearms and explosives transfers based solely on having been placed on a terrorist watch list by federal agents.

[31] Prepared by William J. Krouse, Specialist in Domestic Security and Crime Policy, wkrouse@crs.loc.gov, 7-2225; and Vivian S. Chu, Legislative Attorney, vchu@crs.loc.gov, 7-4576.

[32] From February 2004 through December 2010, out of 1,453 federal firearms-related background checks that resulted in valid terrorist watch list hits, 1,321 (90.9%) were allowed to proceed. U.S. Government Accountability Office, *Update on Firearm and Explosives Background Checks Involving Terrorist Watch List Records*, for the Honorable Frank R. Lautenberg, United States Senate, April 27, 2011, p. 2.

As Senator Susan M. Collins observed in May 2011, however, denying a firearms transfer raises issues, possibly constitutional in nature, that denying an explosives license or permit does not.[33] At the same time, Senators Collins and Joseph I. Lieberman expressed their shared concern about the fact that known and suspected terrorists had passed federal background checks and acquired firearms and explosives legally through normal commercial channels, despite valid terrorist watch list hits.[34] They also noted that Muslim extremists (radicalized jihadists) and other terrorists had used, or had planned to use, firearms and explosives with deadly effect in the past.[35] Such concerns were recently reinforced by Al Qaeda's U.S.-born spokesperson, Adam Gadahn, when he exhorted Muslim extremists in the United States to acquire firearms and carry out terrorist attacks in the United States in a June 2011 Internet posting.[36]

To address such concerns in the 112th Congress, Senator Frank R. Lautenberg and Representative Peter T. King have reintroduced the Denying Firearms and Explosives to Dangerous Terrorists Act of 2011 (S. 34/H.R. 1506).[37] Based on an April 2007 Department of Justice legislative proposal, this bill would authorize the Attorney General to deny a firearms transfer, state-issued firearms permit, or explosives license/permit to any person who has been found "to be or have engaged in conduct constituting, in preparation for, in aid of, or related to terrorism." Supporters have dubbed this legislation the "Terror Gap" proposal; they include 550 mayors of U.S. cities.[38] On the other hand, the National Rifle Association (NRA) and other opponents of the bill argue that the Terror Gap proposal, if enacted, would be unconstitutional, because it would allow the Attorney General to deny a person his "individual right to keep and bear arms," and would do so, "without due process of law."[39] Supporters of the Terror Gap bill counter that it would provide a level of redress and due process that is currently unavailable to others who face a denial of some benefit or activity, because they are identified as known or suspected terrorists through other federal terrorist watch list screening activities.

Continuity of Government Operations[40]

Continuity of government operations refers to programs and initiatives to ensure that governing entities are able to recover from a wide range of potential operational interruptions. Government

[33] *Terrorists and Guns: The Nature of the Threat and Proposed Reforms: Hearing Before the S. Comm. on Homeland Sec. and Gov't Affairs*, 111th Cong. May 5, 2010 (CQ Congressional Transcripts).

[34] Ibid.

[35] Ibid.

[36] Larry McShane, "Terror At Gun Store. U.S. Great Place To Buy Firearms, 'American Al Qaeda' Tells Jihadis," *Daily News (New York)*, June 4, 2011, p. 6.

[37] In addition, during consideration of the FISA Sunsets Reauthorization Act of 2011 (H.R. 1800) in the House Judiciary Committee, Representative Mike Quigley offered an amendment that would have allowed the Attorney General to deny a firearms transfer to any person about whom the Attorney General gathered information during the course of a national security investigation (under FISA), if that information generated a "reasonable belief" that the firearm(s) might be used by the prospective transferee in terrorism-related conduct. This amendment was defeated by a vote of 11 to 21 in full-committee markup.

[38] Letter from Mayors Against Illegal Guns to the Honorable John Boehner, Speaker of the House, and the Honorable Harry Reid, Senate Majority Leader, "*Re: 550 Mayors Call on Congress to Support H.R. 1506/S. 34 and Close the 'Terror Gap,'"* May 11, 2011.

[39] National Rifle Association-Institute for Legislative Action, "Keeping An Eye On 'Terror Watchlist' Legislation, May 20, 2011.

[40] Prepared by R. Eric Petersen, Specialist in American National Government, Government and Finance Division, epetersen@crs.loc.gov, 7-0643.

continuity planning may be viewed as a process that incorporates preparedness capacities, including agency response plans, employee training, recovery plans, and the resumption of normal operations. These activities are established in part to ensure the maintenance of civil authority, provision of support for those affected by an incident, infrastructure repair, and other actions in support of recovery. Arguably, any emergency response presumes the existence of an ongoing, functional government to fund, support, and oversee recovery efforts. Interruptions for which contingency plans might be activated include localized acts of nature, accidents, technological emergencies, and military or terrorist attack-related incidents.

Current authority for executive branch continuity programs is provided in a 2007 National Security Presidential Directive (NSPD) 51 on National Continuity Policy.[41] To support the provision of essential government activities, NSPD 51 sets out a policy "to maintain a comprehensive and effective continuity capability composed of continuity of operations[42] and continuity of government[43] programs in order to ensure the preservation of our form of government[44] under the Constitution and the continuing performance of national essential functions (NEF) under all conditions."

Executive Order (E.O.) 12656, Assignment of Emergency Preparedness Responsibilities, was issued in 1988,[45] and assigns national security emergency preparedness responsibilities to federal executive departments and agencies. E.O. 12656 requires the head of each federal department and agency to "ensure the continuity of essential functions in any national security emergency by providing for: succession to office and emergency delegation of authority in accordance with applicable law; safekeeping of essential resources, facilities, and records; and establishment of emergency operating capabilities." Subsequent sections require each department to carry out specific contingency planning activities in its areas of policy responsibility.

Although contingency planning authorities are chiefly based on presidential directives, Congress could consider whether current authorities accurately reflect current government organization and goals, the costs of these programs, potential conflicts that might result from departments and agencies complying with different authorities, and the extent to which government contingency planning ensures that the federal executive branch will be able to carry out its responsibilities under challenging circumstances.

---

[41] White House, Office of the Press Secretary, *National Security and Homeland Security Presidential Directive*, May 9, 2007, HSPD 51 is also identified as Homeland Security Presidential Directive (HSPD) 20 A more detailed discussion of national continuity policy is available in CRS Report RS22674, *National Continuity Policy: A Brief Overview*, by R. Eric Petersen.

[42] NSPD 51 identifies continuity of operations (COOP) as "an effort within individual executive departments and agencies to ensure that Primary Mission-Essential Functions continue to be performed during a wide range of emergencies, including localized acts of nature, accidents, and technological or attack-related emergencies."

[43] NSPD 51 identifies continuity of government (COG) as "a coordinated effort within the federal government's executive branch to ensure that national essential functions continue to be performed during a catastrophic emergency."

[44] The directive notes "that each branch of the federal government is responsible for its own continuity programs," and requires an executive branch official to "ensure that the executive branch's COOP and COG policies ... are appropriately coordinated with those of the legislative and judicial branches in order to … maintain a functioning federal government." The legislative branch and the federal judiciary maintain continuity programs consonant with their positions as coequal branches of government. NSPD 51 does not specify the nature of appropriate coordination with continuity planners in the legislative and judicial branch.

[45] 53 FR 47491; November 23, 1988.

Federal Building Security: Federal Protective Service[46]

In FY2009, the government's real property[47] comprised over 900,000 assets.[48] The security of this federal property affects not only the daily operations of the federal government but the safety of federal employees and the public. A number of this property is multi-tenant federal buildings that house federal courthouses, and some congressional state and district offices. Security of federal facilities includes physical security assets such as closed-circuit television cameras, barrier material, and security personnel.[49]

The Federal Protective Service (FPS), as the lead "Government Facilities Sector Agency" for the National Infrastructure Protection Plan, is responsible for the protection and security of federally owned and leased buildings, property, and personnel.[50] P.L. 111-83 (FY2010 appropriations for the Department of Homeland Security), transferred FPS from Immigration and Customs Enforcement to the National Protection and Programs Directorate in DHS. In general, FPS undertakes security and law enforcement activities that reduce vulnerability to criminal and terrorist threats, which include all-hazards based risk assessments; emplacement of criminal and terrorist countermeasures, such as vehicle barriers and closed-circuit video cameras; law enforcement response; assistance to federal agencies through facility security committees; and emergency and safety education programs. FPS also assists other federal agencies, such as the U.S. Secret Service at National Special Security Events. Federal agencies protected by FPS pay a fee that is established by the Office of Management and Budget, which has been directed to increase the fee as appropriate to address threats and to adjust the existing fee for FY2011.[51] FPS employs approximately 1,225 law enforcement officers, investigators, and administrative personnel; and it administers the services of approximately 15,000 contract security guards.

Federal facility security practices have been subject to criticism by government auditors and security experts, and have been the topic of congressional oversight hearings.[52] Elements that have received criticism include the use of private security guards, FPS management and security practices, and the coordination of federal facility security. According to FPS, it plans to (1) improve the strategic methods used in identifying and reducing actual and potential threats directed at FPS-protected facilities; (2) restore proactive monitoring activities to mitigate the increased risk to these facilities; (3) improve the service provided by contract security guard forces through acquisition strategies and "intensive" monitoring and training; (4) develop risk-based security standards tied to intelligence and risk-assessments; (5) refine business practices through stakeholder interface; and (6) implement a capital plan that will improve security and

[46] Prepared by Shawn Reese, Analyst in Homeland Security Policy, Government and Finance Division, sreese@crs.loc.gov, 7-0635. For more information on this issue, see CRS Report R41138, *Federal Building, Courthouse, and Facility Security*, by Lorraine H. Tong and Shawn Reese, and CRS Report RS22706, *The Federal Protective Service and Contract Security Guards: A Statutory History and Current Status*, by Shawn Reese.

[47] Real property is defined as property that is leased or owned by the General Services Administration.

[48] U.S. Government Accountability Office, *Federal Real Property: Overreliance on Leasing Contributed to High-Risk Designation*, GAO-11-879T, August 4, 2011, p. 1, http://www.gao.gov/new.items/d11879t.pdf.

[49] These security guards are both federally employed and contracted.

[50] 40 U.S.C. 1315.

[51] Information regarding any changes to FPS or their operations in FY2012 has not been addressed.

[52] U.S. Congress, House Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, *Securing Federal Facilities: Challenges of the Federal Protective Service and the Need For Reform*, 112th Cong., 1st sess., July 13, 2011.

customer service.[53] Congress will likely continue oversight of FPS management and operations in the 112th Congress to ensure that it has the necessary staffing, resources, and funding to carry out its mission.

Judicial and Court Security[54]

By statute 28 U.S.C. §566(a), the U.S. Marshals Service (USMS), within the Department of Justice, has primary responsibility for the security of more than 2,000 sitting federal judges and approximately 5,250 other court officials at over 400 court facilities in the United States and its territories. An appointed U.S. marshal has security responsibility in each of the 94 federal judicial districts and the District of Columbia Superior Court. U.S. marshals provide and oversee security with over 4,500 court security officers (under contract with USMS). According to USMS, threats and inappropriate communications against judges and other protectees have more than doubled from 592 each year in 2003 to approximately 1,400 each year in 2011.[55]

Congress has enacted legislation to improve the safe conduct of court proceedings and to strengthen judicial and court security. For example, Congress passed the Court Security Improvement Act of 2007 (P.L. 110-177), a bill to enhance security for judges, court personnel, and members of the public visiting court facilities (following the murders and violence against judges and their families, and court personnel at the federal and state level in 2005 and 2006[56]). In May 2005, Congress enacted legislation to provide home intrusion detection systems for judges (P.L. 109-13). On March 14, 2011, legislation was introduced (H.R. 1059) to provide permanent authority to the Judicial Conference of the United States for redacting financial disclosure reports filed by a judicial officer or employee if the personal information could compromise the security of the individual or a family member. Current redaction authority, granted under the Ethics in Government Act of 1978, expires at the end of 2011. H.R. 1059 passed the House under suspension of the rules on September 12, 2011.

After a deputy U.S. marshal was wounded and a court security officer was killed at the Lloyd D. George U.S. Courthouse and Federal Building in Las Vegas in January 2010, USMS convened a National Security Review Committee. The committee was tasked to determine whether adequate procedures and practices are in place in courthouses nationwide. USMS has conducted a nationwide review of court security in consultation with the judiciary. The committee's report on the review is expected in September 2011.[57]

[53] U.S. Department of Homeland Security, National Protection & Programs Directorate, President's FY2011 Request *Federal Protective Service: Fiscal Year 2011 Overview, Congressional Justification*, Washington, DC, February 2011, p. FPS-8.

[54] Prepared by Lorraine H. Tong, Analyst in American National Government, Government and Finance Division, ltong@crs.loc.gov, 7-5846. For more information on judicial and court security, see CRS Report R41138, *Federal Building, Courthouse, and Facility Security*, by Lorraine H. Tong and Shawn Reese.

[55] U.S. Marshals Service, *Fact Sheet, Judicial Security 2011*, April 5, 2011, http://www.usmarshals.gov/duties/factsheets/jsd-2011.pdf.

[56] "Judges Plead for Improved Judicial Security," *The Third Branch: Newsletter of the Federal Courts*, Washington, DC, June 2005, pp. 1-2.

[57] USMS provided this information to the author by electronic mail on August 1, 2011.

The workload of the federal courts has increased in almost all case filings. In August 2010, to address the increase of immigration and drug related cases along the U.S. southwest border, Congress appropriated $10 million to the judiciary under P.L. 111-230 (FY2010 emergency supplemental appropriations for border security which also provided $600 million to enhance southwest border security for several executive branch law enforcement agencies). These funds were to be made available until September 30, 2011. In the event more suspects charged with terrorism are tried in federal courts rather than military tribunals, additional security and resources for the courts would be necessary. There could also be a need for greater coordination with local and state law enforcement entities as well as intelligence agencies in such trials. In the 112th Congress, congressional interest will likely continue to ensure that the federal judiciary is provided resources and funding to carry out its constitutional responsibilities.

Food Safety[58]

Intentional contamination of food can result from fraud (e.g., the dilution of a valuable commodity), terrorism, or other harmful intent. Food safety efforts have long focused on preventing common unintentional threats, such as infectious pathogens in poultry or pesticide residues in crops. Since the 2001 terrorist attacks, interest has grown regarding ways to prevent intentional contamination. Large-scale foodborne disease outbreaks can sicken hundreds of people. They can also impose serious economic effects on involved commodities, as well as on uninvolved commodities that the consuming public perceives to be involved. The public's response to the 2001 anthrax attacks and to high-profile unintentional foodborne disease outbreaks suggests that an intentional incident of food contamination, especially if it were an act of terrorism, could have serious economic consequences, in addition to any illnesses it causes.

Federal food safety responsibility rests primarily with the Food and Drug Administration (FDA) and the U.S. Department of Agriculture (USDA). USDA's Food Safety and Inspection Service (FSIS) regulates most meat and poultry and some egg products; FDA is responsible for the safety of most other foods.[59] State and local authorities assist with inspection, outbreak response, and other food safety functions, and regulate retail establishments. DHS notes the complexity of the nation's food and agriculture sector, which accounts for 15% of the nation's economy. In particular, DHS says that "FDA is responsible for the safety of [80%] of all of the food consumed in the United States ... FDA regulates $240 billion of domestic food and $15 billion of imported food. In addition, roughly 600,000 restaurants and institutional food service providers, an estimated 235,000 grocery stores, and other food outlets are regulated by State and local authorities that receive guidance and other technical assistance from FDA."[60]

The 111th Congress enacted a comprehensive food safety law, the Food Safety Modernization Act (FSMA, P.L. 111-353), focused mainly on foods regulated by FDA.[61] FSMA attempts to prevent intentional and unintentional contamination of food through a variety of provisions requiring FDA to develop food safety standards, and requiring food producers and processors to develop

[58] Prepared by Sarah A. Lister, Specialist in Public Health and Epidemiology, slister@crs.loc.gov, 7-7320.

[59] CRS Report RS22600, *The Federal Food Safety System: A Primer*, by Renée Johnson. See also CRS Report R41629, *Food Safety Issues for the 112th Congress*, by Renée Johnson.

[60] DHS, *National Infrastructure Protection Plan: Agriculture and Food Sector Snapshot*, May 2007, http://www.dhs.gov/files/programs/gc_1188565256722.shtm.

[61] CRS Report R40443, *The FDA Food Safety Modernization Act (P.L. 111-353)*, coordinated by Renée Johnson.

comprehensive food safety plans, among others. The law expands FDA's authority to inspect foods and food facilities and to issue recalls, and requires promulgation of regulations to protect against the intentional contamination of food. In addition, FSMA requires the Secretaries of Health and Human Services (HHS) and Agriculture to develop a National Agriculture and Food Defense Strategy, implementation plan, and research agenda, to be consistent with broader national preparedness and response plans.[62]

Implementation of many of FSMA's enhanced regulatory authorities is proceeding.[63] However, some Members of Congress disagree regarding whether activities that would require enhanced FDA funding (such as more frequent FDA inspections of food facilities) are necessary, given budgetary constraints.[64]

Security of Pipelines[65]

Nearly a half-million miles of high-volume pipeline transport natural gas, oil, and other hazardous liquids across the United States.[66] These pipelines are integral to U.S. energy supply and link to other critical infrastructure, such as power plants, airports, and military bases. While a fundamentally safe means of transport, gas and oil pipelines, globally, have been a favored target of terrorists, militant groups, and organized crime. Federal warnings about Al Qaeda also have mentioned pipelines specifically as potential terror targets in the United States.[67] Since September 11, 2001, U.S. officials have foiled plots to attack jet fuel pipelines at the John F. Kennedy International Airport and to attack the Trans Alaska Pipeline System and a major natural gas pipeline in the eastern United States.[68] Notwithstanding these incidents, the most recent U.S. federal threat assessment concludes "with high confidence that the terrorist threat to the U.S. pipeline industry is low ... [with] no specific or credible threat information indicating that violent transnational extremist groups or domestic extremists are actively plotting to conduct attacks on the U.S. pipeline industry."[69] Terrorist tactics are in constant flux, however, and difficult to predict, so such attacks remain a possibility in the future.

Federal pipeline security activities are led by the Pipeline Security Division within the Transportation Security Administration (TSA). To date, these activities have relied upon voluntary industry compliance with federal security guidance and TSA security best practices.

---

[62] Ibid, p. 39.

[63] FDA, "FSMA: Progress Reports," http://www.fda.gov/Food/FoodSafety/FSMA/ucm255893.htm.

[64] See, for example, House debate among Reps. John Dingell, Cynthia Lummis, Jack Kingston, and Frank Pallone regarding consideration of H.R. 2112, appropriations for Agriculture, Rural Development, FDA, and Related Agencies for FY2012, *Congressional Record*, June 15, 2011, p. H-4253 ff.

[65] Prepared by Paul Parkfomak, Specialist in Energy and Infrastructure Policy, Resources, Science and Industry Division, pparfomak@crs.loc.gov, 7-0030.

[66] Hazardous liquids primarily include crude oil, gasoline, jet fuel, diesel fuel, home heating oil, propane, and butane. Other hazardous liquids transported by pipeline include anhydrous ammonia, carbon dioxide, kerosene, liquefied ethylene, and some petrochemical feedstocks.

[67] "Already Hard at Work on Security, Pipelines Told of Terrorist Threat," *Inside FERC*, McGraw-Hill Companies, January 3, 2002.

[68] U.S. Attorney's Office, Middle District of Pennsylvania, "Man Convicted of Attempting to Provide Material Support to Al-Qaeda Sentenced to 30 Years' Imprisonment," Press release, November 6, 2007; U.S. Dept. of Justice, "Four Individuals Charged in Plot to bomb John F. Kennedy International Airport," Press release, June 2, 2007.

[69] Transportation Security Administration, Office of Intelligence, *Pipeline Threat Assessment*, January 18, 2011, p. 3.

TSA has been engaged in a number of specific pipeline security initiatives since 2003, including developing security standards; implementing measures to mitigate security risk; building and maintaining stakeholder relations, coordination, education and outreach; and monitoring compliance with voluntary pipeline security standards. The cornerstone of TSA's pipeline activities is its Corporate Security Review (CSR) program, wherein the agency visits the largest pipeline and natural gas distribution operators to review their security plans and inspect their facilities. TSA has completed CSRs covering the largest 100 pipeline systems (84% of total U.S. energy pipeline throughput) and is in the process of conducting second CSRs of these systems.[70] In 2008, the TSA initiated its Critical Facility Inspection Program (CFI), under which the agency conducts in-depth inspections of all the critical facilities of the 125 largest pipeline systems in the United States. By the end of 2011, TSA expects to complete CFIs for all of these pipeline operators.[71] The agency estimates that these 125 pipeline systems collectively include approximately 600 distinct critical facilities.[72]

While TSA is generally credited with significantly strengthening U.S. pipeline security, Congress has had ongoing concerns about the adequacy of the agency's pipeline security standards, its overall level of resources, and certain aspects of its CSR program. Some Members of Congress, as well as the Department of Transportation's (DOT) Office of Inspector General, have questioned the adequacy of voluntary, rather than mandatory, federal pipeline security requirements.[73] In 2010, a Member expressed concern that TSA's pipeline division—with 13 full-time equivalent staff—did not have sufficient staff to carry out a federal pipeline security program on a national scale.[74] In a 2010 report, the GAO recommended a number of specific actions to improve TSA's pipeline security priority-setting and CSR assessment processes, such as transmitting CSR recommendations in writing to pipeline operators.[75] To date, there has been no federal legislation directly addressing these concerns, but they may receive additional attention in the 112th Congress. In addition to these specific issues, the next Congress may assess how pipeline security fits together with the U.S. pipeline safety program, administered by the DOT, in the nation's overall strategy to protect transportation infrastructure. While the DOT and TSA have distinct missions, pipeline safety and security are intertwined.[76]

[70] Government Accountability Office (GAO), *Pipeline Security: TSA Has Taken Actions to Help Strengthen Security, but Could Improve Priority-Setting and Assessment Processes*, GAO-10-867, August, 2010, Executive Summary.

[71] GAO, August 2010, p. 32.

[72] Department of Homeland Security, " Intent to Request Renewal and Amendment From OMB of One Current Public Collection of Information: Critical Facility Information of the Top 100 Most Critical Pipelines," 76 *Federal Register* 35229, June 16, 2011.

[73] U.S. Dept. of Transportation, Office of Inspector General*, Actions Needed to Enhance Pipeline Security, Pipeline and Hazardous Materials Safety Administration*, Report No. AV-2008-053, May 21, 2008, p. 6.

[74] The Honorable Gus M. Billirakis, Remarks before the House Committee on Homeland Security, Subcommittee on Management, Investigations, and Oversight hearing on "Unclogging Pipeline Security: Are the Lines of Responsibility Clear?," Plant City, FL, April 19, 2010.

[75] U.S. Government Accountability Office, *Pipeline Security: TSA Has Taken Actions to Help Strengthen Security, but Could Improve Priority-Setting and Assessment Processes*, GAO-10-867 August 4, 2010, pp. 56-57.

[76] For further analysis, see CRS Report R41536, *Keeping America's Pipelines Safe and Secure: Key Issues for Congress*, by Paul W. Parfomak.

Security of Chemical Facilities[77]

Congress provided DHS authority to regulate security at chemical facilities in the Homeland Security Appropriations Act, 2007 (P.L. 109-295, Section 550). This authority expires on October 4, 2011. Congressional policymakers are considering a range of actions in the 112th Congress, including an extension or revision of this authority. Various stakeholders have criticized the content of DHS regulation and the pace of its implementation and have recommended changes to the underlying statute. Recommended changes include broadening the regulated community, enabling the federal government to require adoption of particular security measures at facilities, and increasing access to currently confidential vulnerability information. Other stakeholders, including industry representatives, support an extension of the existing authority without any changes.

The DHS regulates chemical facilities for security purposes. The Obama Administration and others have determined that existing regulatory exemptions, such as for community water systems and wastewater treatment facilities, pose potential risks. Environmental and "right-to-know" groups additionally advocate that Congress include requirements for facilities to adopt or identify "inherently safer technologies" and widely disseminate security-related information to first responders and employees. The regulated industry generally opposes granting DHS the ability to require implementation of inherently safer technologies or other specific security measures. They question the maturity and applicability of the inherently safer technology concept as a security measure and cite the need to tailor security approaches for each facility. The Obama Administration has identified potential security concerns if chemical security-related information is more broadly disseminated. Challenges facing policymakers include whether to extend or change the existing statutory authority, whether to mandate consideration or implementation of inherently safer technologies, what the appropriate balance is between protecting security information and releasing information to non-governmental stakeholders, and how to assess and potentially ameliorate costs associated with implementing required security measures.

The DHS regulatory program is still in its early stages and has experienced implementation delays. No chemical facility has yet to fully comply with the DHS chemical security regulations. Significant changes in this program could lead to further delays. In contrast, changes to the regulatory program may be most effective if made early in the program's implementation, rather than later after companies have invested in specific security measures.[78]

Security of Wastewater and Water Utilities[79]

The systems that comprise the nation's water supply and water quality infrastructure have long been recognized as being potentially vulnerable to terrorist attacks of various types, including physical disruption, bioterrorism/chemical contamination, and cyber attack. Across the country, these systems consist of 16,000 publicly owned wastewater treatment facilities and 168,000 public drinking water facilities, plus thousands of miles of pipes, aqueducts, water distribution, and sewer lines. Damage or destruction could disrupt the delivery of vital human services,

[77] Prepared by Dana A. Shea, Specialist in Science and Technology Policy, dshea@crs.loc.gov, 7-6844.

[78] For further CRS research on this issue, consult CRS Report R41642, *Chemical Facility Security: Issues and Options for the 112th Congress*, by Dana A. Shea.

[79] Prepared by Claudia Copeland, Specialist in Resources and Environmental Policy, ccopeland@crs.loc.gov, 7-7227.

threatening public health and the environment, or possibly causing loss of life. In recognition, Congress and other policymakers have considered a number of initiatives in this area, including enhanced physical security of water infrastructure facilities, improved communication and coordination, and research. Recent policy interest has focused on two issues: (1) security of wastewater utilities, and (2) whether to include wastewater and water utilities in chemical plant security regulations implemented by DHS.

When Congress created DHS in 2002,[80] it gave DHS responsibility to coordinate information to secure the nation's critical infrastructure, including the water sector, through partnerships with the public and private sectors. Under Homeland Security Presidential Directive 7, the Environmental Protection Agency (EPA) is the lead federal agency for protecting wastewater and drinking water utility systems, because EPA has regulatory authority over both types of water utilities under the Clean Water Act and the Safe Drinking Water Act, respectively. Separately, in P.L. 107-188,[81] Congress required drinking water systems serving more than 3,300 persons to conduct vulnerability analyses and to submit the assessments to EPA. Since the 108th Congress, congressional committees have considered legislation to encourage or require wastewater treatment facilities to similarly conduct vulnerability assessments and develop site security plans (such as H.R. 2883 in the 111th Congress), but no bill has been enacted.

Congress also has been considering requirements for wastewater and drinking water utilities in connection with legislation to establish risk-based and performance-based security standards at the nation's chemical plants (see discussion of "Security of Chemical Facilities"). Issues debated for some time include (1) whether to preserve an existing exemption for water utilities from chemical facility standards or include them in the scope of DHS rules; and (2) whether water utilities that store or use extremely hazardous substances, such as chlorine gas, should be required to consider the use of different chemicals or safer processes (so-called "inherently safer technology"). A third issue is what roles should EPA and DHS play in implementing such requirements and generally in overseeing homeland security at wastewater and drinking water utilities. There has been considerable debate about coordination between EPA and DHS and whether EPA's lead role for the water utility sector would be altered. Water utilities have urged Congress not to create a dual or split regulatory arrangement between two agencies, arguing that EPA has long-standing expertise in wastewater and water regulatory and security issues. Others have argued that DHS should have overall responsibility.

Legislative proposals addressing these issues in the 112th Congress include H.R. 901, approved by the House Homeland Security Committee in June; H.R. 908, approved by the House Energy and Commerce Committee in May; and S. 473, approved by the Senate Homeland Security and Government Affairs Committee in June. These bills differ in a number of other respects but reflect apparent consensus regarding water utility issues: all of the bills would preserve the existing exemption from DHS chemical facility standards, and none would mandate inherently safer technology. Further, none would alter EPA's lead role for the water utility sector. Separate Senate legislation, S. 711, includes provisions for inherently safer technology and would add coverage of wastewater and drinking water facilities in the DHS rules.

Since the terrorist attacks of 2001, wastewater and water utilities have been engaged in numerous activities to assess potential vulnerabilities and strengthen protections. Congressional oversight of

[80] P.L. 107-297; 116 Stat. 2322.

[81] The Public Health Security and Bioterrorism Preparedness and Response Act, 116 Stat. 594.

this sector's homeland security activities has been limited but could be of interest in the 112th Congress.[82]

Cybersecurity[83]

Cyberspace (the globally integrated system of computers, servers, routers, data centers, etc. and the information and software contained therein) is vulnerable to nefarious activity. Threats may come from state actors, criminal syndicates or individuals, terrorist and other politically motivated groups, industrial competitors, and individuals wanting to test their mettle against efforts to thwart them. The nefarious activities include stealing, modifying, or destroying information or disrupting the flow of information through cyberspace. Possible consequences include loss of financial resources, economic competitiveness, and the ability for federal agencies to carry out their missions or critical infrastructures to produce and deliver needed products. There is also concern that in some cases, stealing, modifying, destroying, or disrupting the flow of information could result in catastrophic failures in industrial processes leading to loss of life, physical property, and environmental quality.

The Department of Homeland Security plays a major role in helping to defend cyberspace, primarily focused on protecting the federal government's non-national security information systems and the information systems of critical infrastructures. However, the range of national risks involved, and the roles and relationships between stakeholders are complex and go beyond the ability of a single agency to address. Current efforts are guided in a large part by the Obama Administration's Cybersecurity Review.

Near term efforts focus on improving defenses – monitoring networks, detecting nefarious activity, responding quickly to that activity once its been detected, and recovering from it. This requires information sharing among stakeholders, awareness programs so all stakeholders are cognizant of the risks, training of skilled cyber security personnel, and quick and agile security management techniques.

Mid-term activities include improving the security of software and products being introduced into the market. This requires analyzing current vulnerabilities and intrusion techniques and introducing development processes to improve the security of products before they come to the market. Mid-term activities also include international treaties, multi-lateral, and bi-lateral cooperation and coordination in criminalizing, investigating and prosecuting cyber perpetrators or international treaties on allowable rules of engagement in cyberspace. Long-term activities include research and development that might lead to new network protocols or architectures that make cyberspace more inherently secure. Another area of study is the restructuring of incentives to favor security.

Both the executive branch and Congress have been active in trying to secure cyberspace for many years. Partnerships have been developed between federal agencies and between the federal government and the private sector, and state, local, tribal, and territorial governments. Both federal and non-federal owners and operators of networks, as well as private firms to which owners and operators have contracted out network security, are monitoring networks and

[82] For additional information, see CRS Report RL32189, *Terrorism and Security Issues Facing the Water Infrastructure Sector*, by Claudia Copeland.

[83] Prepared by John D. Moteff, Specialist in Science and Technology Policy, jmoteff@crs.loc.gov, 7-1435.

communicating with each other. Government and private firms have established cyber response teams. The federal government and private sector are funding R&D, awareness, and training programs. Some issues have received relatively less attention. These include the role of the National Security Agency in protecting critical infrastructures; at what point a cyber intrusion or attack becomes the domain of the Department of Defense (triggering rules of engagement in a cyber conflict); and emergency powers for the President.

During the first session of the 112th Congress, several bills have been proposed that address one or more aspects of the policy issues associated with cybersecurity. Among those bills are H.R. 76, H.R. 174, H.R. 1136, H.R. 2096, S. 372, S. 413, S. 1152, and S. 1342. In July, 2011, the White House, too, proposed legislative language meant to improve cybersecurity. The issues addressed by one or more of these bills include statutory establishment of a high level office that would coordinate cybersecurity policy across the federal government; modification of the current Federal Information Security Management Act and clarification of agencies' roles; penalties for cybercrimes; national standards for breach notification; research and development; and, workforce development. Some of the bills expand into new areas such as considering or requiring private sector owners/operators of critical infrastructure assets to develop cybersecurity plans (S. 372, S. 413, H.R. 174, and the White House proposal) and emergency powers for the President (S. 413). To date only H.R. 2096 has been reported out of committee.

Although none of the bills have made it to either the House or Senate floor, the leadership in both chambers have expressed interest in pursuing comprehensive cybersecurity legislation. Senate Majority Leader Reid's office is heading an effort to draft comprehensive legislation that would cut across committee jurisdiction. The Senate Minority Leader McConnell's office has expressed interest in participating in the effort's working groups.[84] Also, the House Republican leadership has formed a cybersecurity task force to develop legislative language. It is reported that the task force will present its findings to Speaker Boehner by October 2011.

Transit Rail Emergency Preparedness[85]

Each day, on average, some 12 million trips are made using transit rail (i.e., heavy rail, light rail, and commuter rail).[86] While emergency incidents involving transit rail are relatively rare, such incidents can result in extensive injuries and death due to the number of passengers involved. Congress has given TSA responsibility for transit security oversight, and has created a transit security grant program under DHS. The DHS Inspector General's Office recommended that TSA take steps to provide more support to transit rail stakeholders in preparing for and responding to emergencies.[87] Members of the 112th Congress might elect to evaluate these recommendations and consider legislative action.

[84] Diane Bartz, "Reid pushes US Republicans for cybersecurity bill" *Reuters*, July 27, 2011. See, http://www.reuters.com/article/2011/07/27/congress-cybersecurity-idUSN1E76Q1M320110727. Last viewed September 8, 2011.

[85] Prepared by Randy Peterman, Analyst in Transportation Policy, dpeterman@crs.loc.gov, 7-3267.

[86] American Public Transportation Association, *2010 Public Transportation Fact Book*, April 2010, Table 5: Unlinked Passenger Trips by Mode, Millions, http://www.apta.com/resources/statistics/Documents/FactBook/APTA_2010_Fact_Book.pdf; The table gives an annual total; CRS calculated daily trips by dividing the total by 365 days.

[87] Department of Homeland Security, Office of Inspector General, *TSA's Preparedness for Mass Transit and Passenger Rail Emergencies*, OIG-10-68, March 2010, http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_10-68_Mar10.pdf.

The DHS OIG looked at four aspects of TSA's effort to help transit rail stakeholders prepare for and respond to emergencies, and made recommendations for improvements:

- Evaluation of transit agency security practices by TSA inspectors.

  The OIG concluded that TSA's evaluations of agencies' security practices were not consistent and thorough, which made it difficult for TSA and the agencies to develop corrective actions. The OIG recommended that TSA provide better training to its inspectors and implement a new database tool to ensure that the assessments are consistent. TSA said a new training program for its inspectors is being developed, as is an improved database tool.

- Promotion of knowledge sharing and coordination of security efforts among transit rail providers, regional emergency managers, and first responders through the convening of regional workshops by TSA, in cooperation with the Federal Transit Administration (FTA) of the Department of Transportation.

  The OIG found that FTA had funded all but one of the 20 workshops held thus far, although the Memorandum of Understanding says that TSA and FTA will jointly sponsor the workshops. The OIG recommended that TSA provide more funding so that workshops can be held more frequently. TSA responded that they were willing and able to provide more funding, but that FTA had not sought additional support. TSA agreed to provide more support to transit rail preparedness by promoting coordination of transit rail agency efforts with state and federal partners, law enforcement, and first providers.

- Development of training programs by TSA to prepare frontline transit employees for responding to security threats, in cooperation with the Federal Emergency Management Agency:

  The OIG found that 54 of 59 courses were focused on law enforcement management of security incidents, with only a few courses tailored to transit agency personnel and firefighters. The OIG found that no courses were devoted to responding to improvised explosive devices (IEDs). The OIG recommended that TSA offer more courses focused on transit rail operations and on threats posed by IEDs. TSA said that they were developing a more comprehensive training program including courses focused on dealing with the threat of IEDs.

- Organization of regional security exercises by TSA that bring together transit rail providers and first responders to train for prevention of, and response to, acts of terrorism.

  The OIG found that TSA had offered only three intermodal security training exercises for transit rail stakeholders in two years, compared to forty such exercises for port facility stakeholders, and that the transit rail exercises had focused on classroom training. The OIG recommended that TSA offer more intermodal security training exercises that included representatives of transit rail agencies and firefighting agencies, and that these exercises should include live, realistic field drills. TSA said they planned to offer 4 to 6 transit rail exercises in 2010, and planned to include law enforcement officers and other first responders in these exercises, as well as to incorporate live, realistic field drills.

Border Security and Trade

Southwest Border Issues

In recent years, the rising level of violence in communities on the south side of the U.S.-Mexico borders has drawn the attention of the U.S. government and the media. The resulting discussion has touched on a number of issues that have a nexus with homeland security—not just the physical security of the border communities on the U.S. side, but flows of illicit money, trafficking in firearms and continued efforts to thwart development of smuggling tunnels intended to compromise the U.S. border. All of these topics have historically been of interest to Congress—along with the flow of people which is discussed in the Immigration section.

Spillover Violence[88]

There has been an increase in the level of drug trafficking-related violence within and between the drug trafficking organizations (DTOs) in Mexico, and some estimates have placed the number of drug trafficking-related deaths in Mexico at over 34,500 between December 2006 (when Mexican President Felipe Calderón began his campaign against the DTOs) and December 2010.[89] Mexican drug trafficking organizations are now at war with each other as well as with the police and military personnel who are attempting to enforce the drug laws in northern Mexico along the U.S. border. Further, in an illegal marketplace, such as that of illicit drugs, where prices and profits are elevated due to the risks of operating outside the law, violence or the threat of violence becomes the primary means for settling disputes.[90] This has generated concern among U.S. policy makers that the violence in Mexico might spill over into the United States. In particular, an increase in violence in Mexican cities such as Juárez and Nuevo Laredo has sparked fears that the violence may spill into the neighboring U.S. "sister cities" of El Paso and Laredo, TX. For instance, the Department of Homeland Security (DHS) issued a safety alert to law enforcement officers in the El Paso area warning that DTOs and associated gangs may target U.S. law enforcement.[91] U.S. federal officials deny that the recent increase in drug trafficking-related violence in Mexico has resulted in a spillover into the United States, but they acknowledge that the prospect is a serious concern.[92]

The 2010 National Drug Threat Assessment indicates that the Mexican DTOs are the greatest drug trafficking threat to the United States.[93] Mexican DTOs either (1) transport or (2) produce

[88] Prepared by Kristin M. Finklea, Analyst in Domestic Security, kfinklea@crs.loc.gov, 7-6259. For more information on measuring spillover violence, see CRS Report R41075, *Southwest Border Violence: Issues in Identifying and Measuring Spillover Violence*, coordinated by Kristin M. Finklea.

[89] See University of San Diego, Trans-Border Institute, http://justiceinmexico.org/2011/02/07/trans-border-institute-releases-report-on-drug-violence-in-mexico/.

[90] Jeffrey A. Roth, "Psychoactive Substances and Violence," National Institute of Justice (Research in Brief Series), February 1994 (Washington, D.C.: U.S. Department of Justice).

[91] "Department of Homeland Security (DHS): Mexican Assassin Teams Targeting U.S. Law Enforcement," *Homeland Security Newswire*, April 6, 2010.

[92] Ramon Bracamontes, "CBP Chief Assesses the Border: Alan Bersin, in El Paso, Assures Safety, Backs Mexico's Fight," *El Paso Times*, January 6, 2011.

[93] U.S. Department of Justice, National Drug Intelligence Center, *National Drug Threat Assessment 2010,* Product No. 2010-Q0317-001, February 2010, http://www.justice.gov/ndic/pubs38/38661/38661p.pdf.

and transport drugs north across the United States-Mexico border. After being smuggled across the border by DTOs, the drugs are distributed and sold within the United States. The illicit proceeds may then be laundered or smuggled south across the border. The proceeds may also be used to purchase weapons in the United States that are then smuggled into Mexico. The United States is the largest marketplace for illegal drugs and sustains a multi-billion dollar market in illegal drugs—thus partially fueling the threat posed by the DTOs.[94] While drugs are the primary goods trafficked by the DTOs, they also generate income from other illegal activities, such as the smuggling of humans and weapons, counterfeiting and piracy, kidnapping for ransom, and extortion. Reports of these crimes in the United States have contributed to the fear of spillover violence.

One issue that may be of concern to Congress involves determining exactly what constitutes spillover violence above and beyond the level of drug trafficking-related violence that has previously existed in the United States. The interagency community has defined "spillover violence" as violence targeted primarily at civilians and government entities—excluding trafficker-on-trafficker violence[95]—while other experts and scholars have maintained that trafficker-on-trafficker violence is central to spillover.[96] A clear definition of spillover is central to debating policy options to prevent or mitigate such violence. A related issue that Congress may consider is how to prevent drug trafficking-related violence from spilling into the United States. Potential options that experts have presented include increasing border enforcement efforts; providing additional aid to Mexico to support the disruption of organized crime, implementation of judicial reform, enhancement of a 21st century border, and strengthening communities;[97] reducing drug demand in the United States; and decriminalizing or legalizing certain drugs.

Illicit Proceeds and the Southwest Border[98]

The flow of money outside legal channels not only presents challenges to law enforcement, but it also has a significant nexus with homeland security policy. Proceeds from illegal enterprises are sometimes used to fund broader destabilizing activities, such as smuggling, illegal border crossings, or more violent activities, such as the operations of the FARC and right-wing paramilitary groups in Colombia.[99] While this is an issue with a global scope, this section focuses specifically on the policies affected by movement of illicit funds across the Southwest border.

---

[94] Oriana Zill and Lowell Bergman, "Do the Math: Why the Illegal Drug Business is Thriving," *PBS Frontline*, http://www.pbs.org/wgbh/pages/frontline/shows/drugs/.

[95] According to the DEA, "[S]pillover violence entails deliberate, planned attacks by the cartels on U.S. assets, including civilian, military, or law enforcement officials, innocent U.S. citizens, or physical institutions such as government buildings, consulates, or businesses. This definition does not include trafficker on trafficker violence, whether perpetrated in Mexico or the U.S." See Drug Enforcement Administration, *Statement of Joseph M. Arabit Special Agent in Charge, El Paso Division*, Regarding "Violence Along the Southwest Border" Before the House Appropriations Committee, Subcommittee on Commerce, Justice, Science and Related Agencies, March 24, 2009, http://www.usdoj.gov/dea/speeches/s032409.pdf.

[96] Testimony by David Shirk, Director, Trans-Border Institute, University of San Diego, before the U.S. Congress, House Committee on Appropriations, Subcommittee on Commerce, Justice, Science, and Related Agencies, *Federal Law Enforcement Response to US-Mexico Border Violence*, 111th Cong., 1st sess., March 24, 2009.

[97] For more information on U.S. assistance to Mexico and on bilateral security cooperation, see CRS Report R41349, *U.S.-Mexican Security Cooperation: The Mérida Initiative and Beyond* , by Clare Ribando Seelke and Kristin M. Finklea.

[98] Prepared by Kristin M. Finklea, Analyst in Domestic Security, kfinklea@crs.loc.gov, 7-6259.

[99] Office of the Coordinator for Counterterrorism, *Country Reports on Terrorism 2009*, U.S. Department of State, (continued...)

The sale of illegal drugs in the United States generates somewhere between $18 billion and $39 billion in annual wholesale proceeds for Mexican and Colombian drug trafficking organizations (DTOs).[100] Money from the DTOs' illegal sale of drugs in the United States is moved south across the border into Mexico. Moving these funds from the United States into Mexico fuels the drug traffickers' criminal activities. This money is not directly deposited into the U.S. financial system, but rather is illegally laundered through mechanisms such as bulk cash smuggling, the Black Market Peso Exchange[101] (BMPE), or placed in financial institutions, cash-intensive front businesses, prepaid stored value cards (PSVCs), or money services businesses (MSBs).[102]

The National Drug Intelligence Center (NDIC) indicates that the development of new technologies has provided outlets through which DTOs may conceal their illicit proceeds.[103] Increasingly, the use of stored value cards, [104] mobile banking systems, and other technologies, allow traffickers to move profits more quickly and stealthily. In addition, profits that the Mexican DTOs generate from the sale of Colombian cocaine can be moved directly from the United States to the source country without traversing through middlemen.[105]

While bulk cash smuggling has been an important means by which criminals have moved illegal profits from the United States into Mexico, traffickers have increasingly turned to stored value cards to move money. With these cards, criminals are able to avoid the reporting requirement under which they would have to declare any amount over $10,000 in cash moving across the border. Current federal regulations regarding international transportation only apply to monetary instruments as defined under the Bank Secrecy Act.[106] A stored value card is not, however,

(...continued)

Washington, DC, August 5, 2010, http://www.state.gov/s/ct/rls/crt/2009/140888.htm.

[100] U.S. Department of Justice, National Drug Intelligence Center (NDIC), *National Drug Threat Assessment 2009,* Product No. 2008-Q0317-005, December 2008, p.49, http://www.usdoj.gov/ndic/pubs31/31379/31379p.pdf. This is the most recent estimate of total annual proceeds. With respect to bulk cash, the most recent NDIC threat assessment (2010) indicates that from 2003 – 2004, an estimated $17.2 billion was smuggled from the United States to Mexico in the form of bulk cash alone. See U.S. Department of Justice, National Drug Intelligence Center, *National Drug Threat Assessment 2010,* Product No. 2010-Q0317-001, February 2010, p. 47, http://www.justice.gov/ndic/pubs38/38661/38661p.pdf. (Hereafter *NDTA, 2010*).

[101] The Department of the Treasury defines the BPME as "a large-scale money laundering system used to launder proceeds of narcotic sales in the United States by Latin American drug cartels by facilitating swaps of dollars in the U.S. for pesos in Colombia through the sale of dollars to Latin America businessmen seeking to buy U.S. goods to export," http://www.fincen.gov/statutes_regs/guidance/html/advis04282006.html.

[102] According to the Department of the Treasury, a money services business is any person or entity engaging in activities including exchanging currency; cashing checks; issuing, selling, or redeeming travelers' checks, money orders, or stored value; and transmitting money. For more information, see http://www.fincen.gov/financial_institutions/msb/definitions/msb.html.

[103] See *NDTA, 2010*, pp. 47 – 50 for more information on developments in illicit finance.

[104] According to the Code of Federal Regulations, stored value are "funds or monetary value represented in digital electronics format (whether or not specially encrypted) and stored or capable of storage on electronic media in such a way as to be retrievable and transferable electronically," 31 C.F.R. § 103.11(vv).

[105] Douglas Farah, "Money Laundering and Bulk Cash Smuggling: Challenges for the Merida Initiative," in *Shared Responsibility: U.S.-Mexico Policy Options for Confronting Organized Crime*, ed. Eric L. Olson, David A. Shirk, and Andrew D. Selee (2010), p. 144.

[106] 31 U.S.C. § 5312(a)(3) defines a monetary instrument as "(A) United States coins and currency; (B) as the Secretary may prescribe by regulation, coins and currency of a foreign country, travelers' checks, bearer negotiable instruments, bearer investment securities, bearer securities, stock on which title is passed on delivery, and similar material; and (C) as the Secretary of the Treasury shall provide by regulation for purposes of sections 5316 and 5331 , checks, drafts, notes, money orders, and other similar instruments which are drawn on or by a foreign financial institution and are not in bearer form."

considered a monetary instrument under current law, and thus is not subject to these international transportation regulations. Policy makers may debate the proper balance between providing for the ease of legitimate monetary transactions and inhibiting the movement of proceeds from illegal activities.

Various departments and agencies—including the Drug Enforcement Administration, Federal Bureau of Investigation, U.S. Immigration and Customs Enforcement, U.S. Customs and Border Protection, and the Financial Crimes Enforcement Network—share responsibility for combating drug-related activity and the flow of illicit proceeds both along the Southwest border and throughout the United States. Many of these agencies are also represented in Mexico, increasing U.S.-Mexican bilateral cooperation. Further, while some efforts explicitly target money laundering and bulk cash smuggling, other efforts are more tangentially related. For instance, operations targeting southbound firearms smuggling may intercept individuals smuggling not only weapons, but cash proceeds from illicit drug sales as well. http://www.crs.gov/pages/Reports.aspx?PRODCODE=R41547&Source=search - fn110http://www.crs.gov/pages/Reports.aspx?PRODCODE=R41547&Source=search - fn108

Southwest Border Gun Trafficking[107]

Many view illegal gun trafficking from the United States as a significant factor in the escalating drug-related violence in Mexico. To stem the flow of illegal guns, the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) has stepped up enforcement of domestic gun control laws in the four Southwest border states under a program known as "Project Gunrunner." Although the magnitude of the flow of illegal guns from the United States to Mexico is unknown, ATF firearms trace data indicates that such a flow exists. However, it is unclear whether that flow is an "ant run" that has trickled across the border over many years, or an "iron river of guns" that has surged in recent years as Mexico drug traffickers have sought to arm themselves with firearms that are commonly available on U.S. civilian markets. Those firearms include semiautomatic variants of AK-47 and AR-15 rifles, .50 caliber sniper rifles, and 5.7 FN pistols, as well as other semiautomatic pistols and revolvers of various calibers.[108]

In February 2011, Project Gunrunner came under scrutiny for a Phoenix, AZ-based investigation known as "Operation Fast and Furious," when ATF whistleblowers alleged to Members of Congress that suspected straw purchasers were allowed to amass relatively large quantities of firearms as part of a long-term gun trafficking investigation.[109] They alleged further that ATF allowed those firearms to "walk," meaning that ATF allowed known straw purchasers[110] to transfer firearms to gunrunners, without taking additional steps to surveil those suspects, monitor the movement of those firearms, or expeditiously arrest either the suspected straw purchasers or gunrunners. Two of those firearms—AK-47 style rifles—were reportedly found at the scene of a shootout near the U.S.-Mexico border where U.S. Border Patrol Agent Brian Terry was shot to

[107] Prepared by William J. Krouse, Specialist in Domestic Security and Crime Policy, wkrouse@crs.loc.gov, 7-2225; and Vivian S. Chu, Legislative Attorney, vchu@crs.loc.gov, 7-4576.

[108] U.S. Government Accountability Office, *Firearms Trafficking: U.S. Efforts to Combat Arms Trafficking to Mexico Face Planning and Coordination Challenges*, GAO-09-709, June 2009, p. 17 .

[109] James v. Grimaldi and Sari Horwitz, "ATF Probe Strategy Is Questioned," *Washington Post*, February 2, 2011.

[110] A "straw purchase" occurs when a person, who is otherwise eligible to purchase a firearm, purchases a firearm from a federally licensed dealer for another person, who is either prohibited from possessing a firearm or does not want a paper trail linking him to the purchased firearm.

death.[111] Questions, moreover, have been raised about whether a firearm—an AK-47 style handgun—that was reportedly used to murder U.S. ICE Special Agent Jamie Zapata and wound Special Agent Victor Avila in Mexico on February 15, 2011, was initially trafficked by a subject of a Houston, TX-based ATF Project Gunrunner investigation.[112] While it remains an open question whether ATF or other federal agents were in a position to interdict the firearms used in these deadly attacks before they were smuggled into Mexico,[113] neither DOJ nor ATF informed their Mexican counterparts about these investigations and the possibility that some of these firearms could be reaching Mexico.[114]

Cross-Border Smuggling Tunnels[115]

Mexican traffickers rely on the use of cross-border tunnels to smuggle persons and drugs, as well as other contraband, from Mexico into the United States. The use of smuggling tunnels has increased not only in frequency but in the sophistication of the tunnels themselves.[116] More than 150 tunnels have been discovered along the Southwest border since the 1990s.[117] Early tunnels were rudimentary "gopher hole" tunnels dug on the Mexican side of the border, traveling just below the surface, and popping out on the U.S. side as close as 100 feet from the border. Slightly more advanced tunnels to relied on existing infrastructure, which may be shared by neighboring border cities such as the tunnel shared by Nogales, AZ, in the United States and Nogales, Sonora, in Mexico. These interconnecting tunnels may tap into storm drains or sewage systems, allowing smugglers to move drugs further and more easily than in tunnels they dug themselves. The most sophisticated tunnels can have rail, ventilation, and electrical systems. The most extensive of such tunnels discovered to date was found in January 2006 in Otay Mesa, CA, 85 feet below the surface of the earth. It stretched three-quarters of a mile in length, boasted lighting, ventilation and groundwater drainage systems, and its discovery resulted in the seizure of more than two tons of marijuana.[118] In November 2010, the San Diego Tunnel Task Force[119] uncovered two similar tunnels running between Tijuana, Mexico, and Otay Mesa, CA.[120]

---

[111] Ibid.

[112] Ibid.

[113] Operation Fast and Furious was launched in November 2009. It was approved as an Organized Crime and Drug Enforcement Task Force (OCDETF) investigation in February 2010. As an OCDETF investigation, it was then directed largely by the U.S. Attorney's Office in Phoenix. While Immigration and Customs Enforcement (ICE) and Internal Revenue Service (IRS) agents were also part of this investigation, so far their role in this operation has not generated public or congressional scrutiny.

[114] Richard A. Serrano, "U.S. Embassy Kept in Dark as Guns Flooded Mexico," *Salt Lake Tribune*, July 25, 2011.

[115] Prepared by Kristin M. Finklea, Analyst in Domestic Security, kfinklea@crs.loc.gov, 7-6259.

[116] Ken Stier, "Underground Threat: Tunnels Pose Trouble from Mexico to Middle East," *Time*, May 2, 2009.

[117] Statement of James A. Dinkins, Executive Associate Director, Homeland Security Investigations, U.S. Immigration and Customs Enforcement, before the U.S. Congress, Senate United States Senate Caucus on International Narcotics Control, *Illegal Tunnels on the Southwest Border*, 112th Cong., 1st sess., June 15, 2011.

[118] U.S. Drug Enforcement Administration, "DEA/ICE Uncover 'Massive' Cross-Border Drug Tunnel, Cement lined passage thought to link warehouses in Tijuana and Otay Mesa," press release, January 26, 2006, http://www.justice.gov/dea/pubs/pressrel/pr012606.html.

[119] This Task Force was created in 2003 as a partnership between ICE, DEA, and the USBP, along with state law enforcement and Mexican counterparts.

[120] U.S. Drug Enforcement Administration, "Discovery of 2nd Major San Diego-Area Cross-Border Drug Tunnel Leads to 8 Arrests, Seizure of More Than 20 Tons of Marijuana," press release, November 26, 2010, http://www.justice.gov/dea/pubs/states/newsrel/2010/sd112610.html.

U.S. law enforcement uses various tactics to detect these cross-border tunnels. Law enforcement may use sonic equipment to detect the sounds of digging and tunnel construction and seismic technology to detect blasts that may be linked to tunnel excavation. Another tool for tunnel detection is ground penetrating radar.[121] However, factors including soil conditions, tunnel diameter, and tunnel depth can limit the effectiveness of this technology.

Despite these tools, U.S. officials have acknowledged that law enforcement currently does not have technology that is reliably able to detect sophisticated tunnels.[122] Rather, tunnels are more effectively discovered as a result of human intelligence and tips. U.S. officials have noted the value of U.S. – Mexican law enforcement cooperation in detecting, investigating, and prosecuting the criminals who create and utilize the cross-border tunnels.[123] As a result, the 112th Congress may not only consider how to best help U.S. law enforcement develop technologies that can keep pace with tunneling organizations, but also examine whether existing bi-national law enforcement partnerships are effective and whether they may be improved to enhance investigations of transnational criminals.

Cargo Security[124]

Approximately 9.8 million maritime cargo containers arrived at our nation's seaports in 2009, down from a high point of 11.7 million in 2006.[125] In an effort to strike a balance between securing America's borders and facilitating legitimate trade, U.S. Customs and Border Protection (CBP) employs a layered security approach to screen the large number of containers. The approach is centered on advance intelligence, effective inspections, a secure port environment, and international screening of cargo.

In 2006, the Security and Accountability for Every Port Act of 2006 (SAFE Port Act) (P.L. 109-347) directed the Department of Homeland Security (DHS), in coordination with the Department of Energy (DOE), the private sector, and foreign governments, to pilot an integrated system in three foreign ports to scan 100% of containers destined for the United States from those ports. In 2007, section 1703 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Act) (P.L. 110-53) amended the SAFE Port to require that 100% of containers originating outside the United States and unloaded at a U.S. seaport undergo a screening to identify high-risk containers; that 100% of containers that have been identified as high-risk are scanned or searched before such containers leave a U.S. seaport facility; and that 100% of containers loaded on a vessel in a foreign port bound for the United States (either directly or via a foreign port) shall not enter the United States unless the container was scanned by non-intrusive imaging equipment and radiation detection equipment at the foreign port before it is loaded on a vessel.[126] The law requires 100% screening to be implemented by July 2012, but permits the Secretary of Homeland Security to extend the deadline under certain conditions.

[121] For more information, see http://www.geophysical.com/militarysecurity.htm.

[122] Statement of Laura E. Duffy, U.S. Attorney, Southern District of California, U.S. Department of Justice, before the U.S. Congress, Senate United States Senate Caucus on International Narcotics Control, *Illegal Tunnels on the Southwest Border*, 112th Cong., 1st sess., June 15, 2011.

[123] Ibid.

[124] Prepared by Marc R. Rosenblum, Specialist in Immigration Policy, mrosenblum@crs.loc.gov, 7-7360.

[125] U.S. Bureau of Transportation Statistics, "Container Entries into the United states from All Countries and by All Modes: 2000-2009," http://www.bts.gov/publications/americas_container_ports/2011/html/table_07.html

[126] P.L. 109-347, Section 232(a).

Concerns have been raised about the effectiveness and the feasibility of the 100% screening requirement for incoming U.S. cargo. Many have argued that the physical imaging and radiation screening of millions of containers bound for the United States is unrealistic. Others note that the scanning requirement takes only radioactive threats into account, but that a biological weapon is a more likely weapons of mass destruction (WMD) scenario.[127] CBP maintains that its use of a layered, risk-based approach to maritime and cargo security—including the use of advanced electronic information and automated systems to conduct risk-assessments, human resources and technology to inspect and scan all high-risk cargo, and partnerships with the trade community and foreign governments—ensures the security of the supply chain and protects against the introduction of WMD to the United States.[128]

Two cargo screening programs are at the core of this layered approach. The Container Security Initiative (CSI) uses automated targeting tools, strategic intelligence, and CBP officers stationed in foreign ports to identify high-risk containers. High-risk containers receive additional screening by large-scale X-ray and gamma ray machines and radiation detection devices before they are loaded on U.S.-bound ships. CSI was operational in 58 ports in FY2011, and screened over 80 percent of the volume of maritime containers destined for the United States.[129]

Second, pursuant to the SAFE Port Act, three federal agencies—DHS, DOE's National Nuclear Security Administration, and the Department of State—launched the Secure Freight Initiative (SFI) in December 2006; and DHS established the SFI International Container Security pilot program. Under the SFI pilot program, 100% of containers at participating ports are scanned by radiation portal monitors and non-intrusive inspection imaging systems as they move through the ports. Data from these systems are provided to CBP officers stationed at the ports and within the United States at the National Targeting Center-Cargo (NTC-C). CBP officers determine if containers should be referred for secondary examination.

The Administration has requested reductions to CSI and SFI in each of the last two funding cycles, including a 49% reduction from the FY2011 base funding level as a technical adjustment and a 58% reduction in overall funding for FY2012.[130] Based on the initial SFI pilot, CBP concluded that 100 percent scanning of U.S.-bound maritime containers is possible on a limited scale in low volume ports, but that "this process will be difficult to achieve" in many ports and in the case of many transshipped goods.[131] Thus, the Administration proposes to remove CBP officers from most CSI ports and to rely more heavily on remote risk-based targeting at the NTC-C and reciprocal inspections agreements with foreign governments.[132]

In light of the Administration's plans to scale back 100% screening through the SFI pilots, Congress may be interested in the degree to which the NTC-C is positioned to support the

[127] Colonel Randall Larsen, Executive Director of the U.S. Congress Commission on the Prevention of Mass Destruction Proliferation and Terrorism, quoted in Rob Margetta, "Maritime Cargo Screening: The Wrong Approach for Avoiding Nuclear Attack?," *Congressional Quarterly Homeland Security*, Aug. 19, 2010, http://homeland.cq.com/hs/display.do?docid=3724840&sourcetype=31.

[128] U.S. Customs and Border Protection, Report to Congress on Integrated Scanning System Pilots (SAFE Port Act of 2006, Section 231), p. 7, http://www.apl.com/security/documents/sfi_finalreport.pdf. Hereafter: CBP SAFE Port Act Report to Congress.

[129] U.S. Customs and Border Protection, *Congressional Budget Justifications* FY2012, CBP-S&E–37.

[130] Ibid., p. CBP-S&E-32.

[131] CBP SAFE Port Act Report to Congress, p. 9.

[132] U.S. Customs and Border Protection, *Congressional Budget Justifications* FY2012, CBP-S&E–51.

increase in workload that will result from the proposed changes to CSI. Congress may also wish to examine the impact the proposed changes will have on the security of U.S.-bound containers arriving in the United States from CSI ports. Also of possible interest is the degree to which these proposed reductions represent a change in cargo security strategy from one focused on the congressionally-mandated 100% scanning requirement to a remote screening posture focused on high-risk shipments.

Domestic Nuclear Detection[133]

Congress has emphasized the need to detect and interdict smuggled nuclear and radiological material before it enters the United States, funding investment in nuclear detection domestically and abroad. The DHS has adopted a strategy of securing the border through emplacement of radiation portal monitors and non-intrusive imaging equipment. Experts have criticized this combined system as being insufficient to detect all smuggled special nuclear material. The DHS has spent several years developing, testing, and evaluating next-generation detection equipment. The development of these next-generation systems, the Advanced Spectroscopic Portal and the Cargo Advanced Automated Radiography System, has not met testing and evaluation milestones and has lagged performance and timeline expectations.

The DHS has deployed radiation portal monitors and other nuclear and radiological material detection equipment since its establishment. In 2005, DHS established a new office, the Domestic Nuclear Detection Office (DNDO), to research, develop, and procure needed necessary detection equipment and coordinate nuclear detection activities located mainly in Customs and Border Protection, U.S. Coast Guard, and the Transportation Security Administration. The Government Accountability Office (GAO) and other groups have questioned the efficacy of DNDO's efforts to develop a next-generation radiation detection system. Congress has annually barred full-scale procurement of this system until the DHS Secretary certifies that it will provide a significant increase in operational effectiveness relative to existing detection equipment. In July 2011, DHS announced that it would not procure this system.

Congress also has required DHS to scan all containerized cargo entering the United States for nuclear and radiological material. The DHS has not yet met this requirement, and stakeholders question whether the DHS approach will meet this requirement in the future. In addition, a shortfall of a key neutron detection material, helium-3, may force a reconsideration of the current nuclear detection approach, either through development of new neutron-detection materials or through refitting deployed systems with less advantageous neutron-detection capabilities.

DHS activities to detect smuggled radiological and nuclear materials at the U.S. border are part of a large interagency effort to develop a global nuclear detection architecture (GNDA). Congress made DHS, through DNDO, responsible for coordinating federal efforts within the GNDA and implementing this architecture domestically. A GNDA strategic plan has recently been released. The GAO has identified weaknesses in the strategic plan, and they and others await the release of a domestic implementation plan for the GNDA.

The 112th Congress may continue its oversight over the development, testing, and procurement of current and next-generation nuclear detection equipment, interagency coordination in nuclear

[133] Prepared by Dana A. Shea, Specialist in Science and Technology Policy, dshea@crs.loc.gov, 7-6844.

detection, the sufficiency of the global nuclear detection architecture that links this equipment together, and DHS's approach to the helium-3 shortage.[134]

Port Security[135]

The bulk of U.S. overseas trade is carried by ships and thus the economic consequences of a maritime terrorist attack could be significant. A key challenge for U.S. policy makers is prioritizing maritime security activities among a virtually unlimited number of potential attack scenarios. There are far more potential attack scenarios than likely ones, and far more than could be meaningfully addressed with limited counter-terrorism resources. In addition to the 100% container scanning requirement (see discussion above under "Cargo Security"), other port security-related issues before Congress include ongoing implementation of a port worker security card, addressing the threat posed by small craft, and progress towards establishing harbor interagency operational centers.

On January 25, 2007, TSA and the Coast Guard issued a final rule implementing the Transportation Worker Identification Credential (TWIC) at U.S. ports.[136] Longshoremen, port truck drivers, merchant mariners, and other workers entering a port must apply for a TWIC card to obtain unescorted access to port facilities or vessels. The card uses biometric technology for positive identification and TSA conducts a security threat assessment of each worker before issuing a card. The security threat assessment uses the same procedures and standards established by TSA for truck drivers carrying hazardous materials, including examination of the applicant's criminal history, immigration status, mental incapacity, and links to terrorist activity to determine whether a worker poses a security threat. A worker pays a fee of about $133 that is intended to cover the cost of administering the cards. Port facility operators will be responsible for deploying card readers at the gates to their facilities. TSA has tested card readers at a handful of ports to determine the best kind of card reader technology to require. A recent GAO audit found internal control weaknesses in the enrollment, background checking, and use of the TWIC card at ports, which were said to undermine the effectiveness of the credential in screening out unqualified individuals from obtaining access to port facilities.[137]

The use of smaller vessels by terrorists to smuggle weapons or themselves onto U.S. shores or to conduct suicide bombings against larger cargo or passenger ships, similar to the attacks on the *U.S.S. Cole* and the French oil tanker *M/V Limburg*, is a concern. There are too many smaller boats for the Coast Guard to track, and recreational boaters oppose tracking because of the cost of transponders and privacy concerns.[138] Even if small vessels were tracked, there is skepticism about the Coast Guard's ability to thwart an attack given that small vessels routinely sail near potential targets in busy harbor environments. Based on a DHS strategy report, it appears the

[134] For further CRS research on this issue, consult CRS Report RL34750, *The Advanced Spectroscopic Portal Program: Background and Issues for Congress*, by Dana A. Shea, John D. Moteff, and Daniel Morgan.

[135] Prepared by John Frittelli, Specialist in Transportation Policy, jfrittelli@crs.loc.gov, 7-7033.

[136] *Federal Register*, v. 72, no. 16, January 25, 2007, pp. 3492 - 3604.

[137] GAO, *Transportation Worker Identification Credential – Internal Control Weaknesses Need to Be Corrected to Help Achieve Security Objectives,* May 2011, GAO-11-657.

[138] Statement of Margaret Podlich, Boat Owners Association, Subcommittee on Coast Guard and Maritime Transportation, House Committee on Transportation and Infrastructure, Hearing on Maritime Domain Awareness, December 9, 2009.

Coast Guard has no immediate plans to require smaller vessels be outfitted with transponders but will continue to pursue methods to identify small craft.[139]

The Coast Guard is establishing interagency operational centers in major U.S. ports where federal and local law enforcement agencies can share maritime intelligence and coordinate responses when the need arises, such as boarding higher risk vessels.[140] The Coast Guard is planning to co-locate these centers with existing Vessel Traffic Service (VTS) stations where Coast Guard "watch-standers" track and monitor ship movements in a harbor for safety purposes. While these command centers appear to facilitate efforts by law enforcement agencies to "connect the dots" in the maritime environment, Congress has been concerned with the pace at which the Coast Guard is setting up these centers.

Aviation Security[141]

Following the 9/11 terrorist attacks, Congress took swift action to create the Transportation Security Administration (TSA), federalizing all airline passenger and baggage screening functions and deploying large numbers of armed air marshals on commercial passenger flights. TSA remains specifically focused on screening passengers, baggage, and air cargo for explosives and other threats, and considerable challenges remain in effectively screening for explosive threats. Additionally, challenges remain regarding the effective use of watchlists and intelligence information to detect and deter individuals who may pose a threat to civil aviation. Challenges also remain in developing effective strategies and technologies for protecting commercial airliners from attacks by shoulder-fired missiles and other standoff weapons. Finally, challenges remain regarding effective regulation and oversight of airport security measures and access control technologies and procedures.

Explosives Screening Strategy for the Aviation Domain[142]

Prior to the 9/11 attacks, explosives screening in the aviation domain was limited in scope and focused on selective screening of checked baggage placed on international passenger flights. Immediately following the 9/11 attacks, the Aviation and Transportation Security Act (ATSA, P.L. 107-71) mandated 100% screening of all checked baggage placed on domestic and international passenger flights to and from the United States. In addition, the Implementing the 9/11 Commission Recommendations Act of 2007 (P.L. 110-53) mandated the physical screening of all cargo placed on passenger flights. While TSA has met the requirement for cargo screening domestically, largely through implementation of its Certified Cargo Screening Program to oversee screening at off-airport shipping and consolidation facilities combined with supply chain security measures, additional work is needed to implement similar measures for U.S.-bound international flights.[143] Although TSA has yet to fully implement 100% screening of cargo placed on international flights, recent attention has particularly focused on improving explosives screening of passengers in response to continued threats.

---

[139] DHS, *Small Vessel Security Strategy,* April 2008. For a critical review of this strategy, see DHS OIG, *DHS's Strategy and Plans to Counter Small Vessel Threats Needs Improvement,* September 2009.

[140] IOCs were authorized in the Security and Accountability for Every Port Act of 2006 (P.L. 109-347, sec. 108).

[141] Prepared by Bart Elias, Specialist in Aviation Policy, belias@crs.loc.gov, 7-7771.

[142] Prepared by Bart Elias, Specialist in Aviation Policy, belias@crs.loc.gov, 7-7771.

[143] See CRS Report R41515, *Screening and Securing Air Cargo: Background and Issues for Congress*, by Bart Elias.

On December 25, 2009, Umar Farouk Abdulamutallab, a 23-year-old Nigerian, attempted to detonate an explosive device concealed in his underwear aboard Northwest Airlines flight 253 during its approach to Detroit, MI. Al-Qaeda in the Arabian Peninsula claimed responsibility. Al-Qaeda and its various factions have maintained a particular interest in attacking U.S.-bound airliners. Since 9/11, Al-Qaeda has been linked to a plot to bomb several trans-Atlantic flights departing the United Kingdom for North America in 2006 and to the Richard Reid shoe bombing incident aboard American Airlines flight 63 en route from Paris to Miami on December 22, 2001. In response to the Northwest Airlines flight 253 incident, the Obama administration accelerated deployment of Advanced Imaging Technology (AIT) whole body imaging (WBI) screening devices and other technologies at passenger screening checkpoints. This deployment responds to the 9/11 commission recommendation to improve the detection of explosives on passengers.[144]

In addition to AIT, next generation screening technologies for airport screening checkpoints include advanced technology x-ray systems for screening carry-on baggage, bottled liquids scanners, cast and prosthesis imagers, shoe scanning devices, and portable explosives trace detection equipment. The use of AIT has raised a number of policy questions. Privacy advocates have objected to the intrusiveness of AIT, particularly if used for primary screening.[145] The screening of children, the elderly, and individuals with medical conditions and disabilities has been particularly contentious. Recent modifications to pat-down screening procedures, involving more detailed inspection of private areas, have also raised privacy concerns.[146] To allay privacy concerns, TSA currently requires remote screening of images outside of public view and forbids recording or storage of AIT images. It has also begun implementing automated threat detection capabilities that will eliminate the need for TSA screeners to view AIT-generated images.

Other concerns about AIT include the amount of time it takes to screen passengers and the potential medical risks posed by backscatter x-ray systems, despite assurances that the radiation doses from screening are comparatively small. Some have advocated for risk-based use of AIT, perhaps in coordination with a program such at the recently announced trusted traveler test program scheduled to begin in the fall of 2011. Past legislative proposals have specifically sought to prohibit the use of WBI technology for primary screening (see, e.g., H.R. 2200, 111th Congress).[147]

The Use of Terrorist Watchlists in the Aviation Domain[148]

The failed bombing attempt of Northwest Airlines flight 253 on December 25, 2009, also raised policy questions regarding the effective use of terrorist watchlists and intelligence information to identify individuals that may pose a threat to aviation. Specific failings to add the suspect to

[144] National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report*, New York, NY: W. W. Norton & Co., 2004.

[145] See, e.g., American Civil Liberties Union. ACLU Backgrounder on Body Scanners and "Virtual Strip Searches," New York, NY., January 8, 2010.

[146] Donna Goodison, "Passengers Shocked by New Touchy-Feely TSA Screening," *The Boston Herald,* August 24, 2010.

[147] For further reading see CRS Report R40543, *Airport Passenger Screening: Background and Issues for Congress*, by Bart Elias, and CRS Report R41502, *Changes in Airport Passenger Screening Technologies and Procedures: Frequently Asked Questions*, by Bart Elias.

[148] For additional information see CRS Report RL33645, *Terrorist Watchlist Checks and Air Passenger Prescreening*, by William J. Krouse and Bart Elias.

either the no-fly or selectee list, despite intelligence information gathered prior to the flight suggesting that he potentially posed a security threat, prompted reviews of the intelligence analysis and terrorist watchlisting processes. Adding to these concerns, on the evening of May 3, 2010, New York Times Square attempted bombing suspect Faisal Shazad was permitted to board an Emirates Airline flight to Dubai at the John F. Kennedy International airport, even though his name had been added to the no-fly list earlier in the day. He was subsequently identified, removed from the aircraft, and arrested after the airline forwarded the final passenger manifest to CBP's National Targeting Center just prior to departure.[149] Subsequently, TSA modified security directives to require airlines to check passenger names against the no-fly list within two hours of being electronically notified of a urgent update, instead of allowing 24 hours to recheck the list. The event also prompted calls to accelerate the ongoing transfer of watchlist checks from the airlines to the TSA under the Secure Flight program, a process which has now been completed.

By the end of November 2010, the DHS announced that 100% of passengers flying to or from U.S. airports are being vetted using the Secure Flight system.[150] Secure Flight continues the no-fly and selectee list practices of vetting passenger name records against a subset of the Terrorist Screening Database (TSDB). These practices, designed to strike a balance between detecting threats and minimizing false positives, have been criticized because they do not check each passenger against the full set of available government data on potential terrorist threats. Central issues surrounding the Secure Flight program and the use of terrorist watchlists in the aviation domain that may be considered during the 112th Congress include the timeliness of updating watchlists as new intelligence information becomes available; the extent to which complete terrorist information available to the federal government is exploited to assess possible threats among airline passengers and airline and airport workers; the ability to detect potential identity fraud or other attempts to circumvent terrorist watchlist checks, including the potential use of biometrics; the adequacy of established protocols for providing redress to individuals improperly identified as potential threats by watchlist checks; and the adequacy of coordination with international partners.

Recent months have seen renewed efforts to establish a trusted traveler program, intended to offer participants expedited screening. TSA asserts that the program will allow it to focus resources on passengers more likely to pose a risk. A similar test program, called the Registered Traveler program, which involved private vendors that issued and scanned participants' biometric credentials, was scrapped because it failed to show a demonstrable additional security benefit. The planned trusted traveler program aims to build upon existing CBP trusted traveler programs and airline frequent flyer programs.[151] Questions remain regarding whether such a program will be an effective tool to assist in directing security resources to unknown or elevated risk travelers while expediting the screening of program participants.

In addition to these various efforts to screen passengers based on biographic information and biometric data, TSA has invested heavily in developing a passenger behavior detection program to indentify potential threats based on observed behavioral characteristics. In addition to employing observational techniques, TSA Behavior Detection Officers are field testing more

[149] Scott Shane, "Lapses Allowed Suspect to Board Plane," *The New York Times*, May 4, 2010.

[150] Department of Homeland Security. DHS Now Vetting 100 Percent Of Passengers On Flights Within Or Bound For U.S. Against Watchlists, Press Release, November 30, 2010.

[151] Transportation Security Administration, *Expedited Screening Pilot,* http://www.tsa.gov/what_we_do/escreening.shtm.

extensive passenger interviews based on methods employed at Israeli airports.[152] Questions remain regarding the effectiveness of the behavioral detection program, and privacy advocates have cautioned that it could devolve into racial or ethnic profiling of passengers despite concerted efforts to focus solely on behaviors rather than individual passenger traits or characteristics.

Mitigating the Threat of Shoulder-Fired Missiles to Civilian Aircraft[153]

The threat to civilian aircraft posed by shoulder-fired missiles or other standoff weapons capable of downing an airliner, remains a vexing concern for aviation security specialists and policymakers. The threat was brought into the spotlight by the November 2002 attack on a chartered Israeli airliner in Mombasa, Kenya. In 2003, then-Secretary of State Colin Powell remarked that there was "no threat more serious to aviation."[154] Since then, Department of State and military initiatives seeking voluntary reductions of man-portable air defense systems (MANPADS) stockpiles have reduced worldwide inventories by at least 30,000.[155] Despite this progress, an unknown number of such weapons may still be in the hands of insurgents. This threat, combined with the limited capability to improve security beyond airport perimeters and to modify flight paths, leaves civil aircraft vulnerable to missile attacks, especially in conflict zones and other high-risk areas.

The most visible DHS initiative to address the threat was the multiyear Counter-MANPADS program carried out by the DHS Science &Technology Directorate. The program concluded in 2009 with extensive operational and live-fire testing along with FAA certification of systems from two vendors capable of protecting airliners against heat-seeking missiles. The systems have not been operationally deployed on commercial airliners, however, due largely to the high acquisition and life-cycle costs of these units. Some critics have also pointed out that the units do not protect against the full range of potential weapons that pose a potential threat to civil airliners. Proponents, however, argue that the systems do appear to provide effective protection against what is likely the most menacing standoff threat to civil airliners: heat-seeking MANPADS. Nonetheless, the airlines, which continue to face economic difficulties, have not voluntarily invested in these systems for operational use and argue that the costs for such systems should be borne, at least in part, by the federal government. Policy discussions have focused mostly on whether to fund the acquisition of limited numbers of the units for use by the Civil Reserve Aviation Fleet, civilian airliners that can be called up to transport troops and supplies for the military. Other approaches to protecting aircraft, including ground-based missile countermeasures and escort planes or drones equipped with antimissile technology, have been considered on a more limited basis, but these options face operational challenges that may limit their effectiveness.

At the airport level, improving security and reducing the vulnerability of flight paths to potential MANPADS attacks continues to pose unique challenges. While major airports have conducted vulnerability studies, and many have partnered with federal, state, and local law enforcement agencies to reduce vulnerabilities to some degree, these efforts face significant challenges because of limited resources and large geographic areas where aircraft are vulnerable to attack.

[152] Katie Johnston, "A Question for You," *The Boston Globe,* August 3, 2011.

[153] Prepared by Bart Elias, Specialist in Aviation Policy, belias@crs.loc.gov, 7-7771.

[154] Katie Drummond, "Where Have All the MANPADS Gone?" *Wired,* February 22, 2010.

[155] Ibid.

While considerable attention has been given to this issue in years past, considerable vulnerabilities remain, and any terrorist attempts to exploit those vulnerabilities could quickly escalate the threat of shoulder-fired missiles to a major national security priority.

Airport Access Controls and Physical Security[156]

Whereas passenger and baggage screening are carried out by TSA, airports are directly responsible for airport physical security and access control measures. This includes perimeter security, access control systems and badges for secured and restricted areas, surveillance, law enforcement support, and so on. The adequacy of airport access control measures, physical security of airport properties, and TSA oversight of airport security programs has been under scrutiny following a rash of security breaches in 2010. Notably, on January 3, 2010, Haisong Jiang bypassed security at Newark Liberty Airport in New Jersey by entering the sterile area of a passenger terminal through an exit lane that was left unguarded by a transportation security officer. The incident resulted in the evacuation of the terminal, which remained closed for six hours. The policy response to the incident focused primarily on increasing penalties for violators who breach security measures and gain unauthorized access to sterile and secured areas of airports and aircraft. On August 19, 2010, a man being chased by police crashed a stolen pickup truck through a perimeter gate at Dallas Love Field in Texas and drove onto the air operations area, forcing the closure of the airport to flight operations. The incident raised concerns over the adequacy of perimeter access control measures as well as airport security response. Additionally, on August 31, 2010, a woman was shot and killed by police after allegedly making threats with a firearm outside a Delta Airlines maintenance facility at the Atlanta Hartsfield Jackson International Airport in what was described as a domestic situation. While none of these incidents was tied to terrorism, this string of unrelated events has raised policy concerns regarding the implementation and regulatory oversight of airport access controls and physical security measures.

In 2010, concern over firearms at airports also became an issue of considerable debate following consideration of state legislation in Georgia to allow the carriage of firearms in public transit facilities, including commercial airport terminals. The state law would have superseded local ordinances banning firearms carriage in airport terminals. It was not enacted, but prompted debate at the federal level over whether to ban firearms in the non-sterile areas of all commercial airport terminals.

The smuggling of firearms past security checkpoints and onto flights at Orlando International Airport in 2007 prompted considerable concern over the lack of physical screening of airport workers. Preventing airport workers from introducing threats, including weapons and explosives, into the sterile and secured areas of airports has proven difficult. The current TSA approach includes statutory background checks for workers coupled with random and targeted screenings. TSA has tested various screening concepts under its Aviation Direct Access Screening Program (ADASP) and carried out tests to compare these methods to 100% screening. GAO, however, found that design limitations and poor documentation of the pilot program prevented any conclusions from being reached.[157] TSA maintains that random and targeted screening of airport

[156] Prepared by Bart Elias, Specialist in Aviation Policy, belias@crs.loc.gov, 7-7771.

[157] Government Accountability Office. *Aviation Security: A National Strategy and Other Actions Would Strengthen TSA's Efforts to Secure Commercial Airport Perimeters and Access Controls*. GAO-09-399, September 30, 2009.

workers, coupled with statutory background check requirements, provides an adequate level of security.

Identity authentication of various groups including airport workers, airline workers, and law enforcement officers authorized to carry weapons in airport sterile areas and on aircraft has also proven difficult. While crew identification systems for commercial airline pilots and law enforcement officers are being tested at various sites, TSA currently has no plans to implement universal access credentials to airline and airport workers, leaving it up to individual airports to issue access credentials and develop and maintain TSA-approved access control systems.

Also, security procedures affecting general aviation facilities have been controversial and have raised a number of issues regarding credentialing and background check requirements, particularly for transient aircraft operators. General aviation operators often must go through redundant background checks and credentialing processes at multiple airports. TSA has implemented guidance allowing transient operators to gain escorted access to their aircraft and to other airport facilities, but multiple credentials are often needed when crews utilize specific airports on a more regular basis.

Immigration[158]

Immigration policy is multi-tiered and has a variety of key elements: border control and visa security; legal immigration; documentation and verification; interior immigration enforcement; integration, status, and benefits; and refugees and other humanitarian populations.[159] This portion of the report summarizes several immigration issues related to boder security and passenger screening at ports of entry by U.S. Customs and Border Protection (CBP), the agency within DHS within DHS responsible for these activities.[160]

Screening at Ports of Entry[161]

At ports of entry, CBP's Office of Field Operations (OFO) is responsible for conducting immigration, customs, and agricultural inspections of travelers seeking admission to the United States. The vast majority of people entering through U.S. ports are U.S. citizens, U.S. lawful permanent residents (LPRs), and other legitimate visitors. Thus, the overarching task for CBP officers is to identify and intercept dangerous or unwanted (high-risk) people or goods, while facilitating access for legitimate (low-risk) travelers and commerce. CBP seeks to accomplish these screening tasks without excessive infringement on privacy or civil liberties and while controlling enforcement costs.

[158] Prepared by Marc R. Rosenblum, Specialist in Immigration Policy, mrosenblum@crs.loc.gov, 7-7360.

[159] For summaries of legislative activity in recent years, see CRS Report R40848, *Immigration Legislation and Issues in the 111th Congress*, coordinated by Andorra Bruno; CRS Report RL34204, *Immigration Legislation and Issues in the 110th Congress*, coordinated by Andorra Bruno; CRS Report RL33125, *Immigration Legislation and Issues in the 109th Congress*, coordinated by Andorra Bruno; and CRS Report RL32169, *Immigration Legislation and Issues in the 108th Congress*, by Andorra Bruno et al.

[160] For a fuller discussion of immigration issues, see CRS Report R41704, *Overview of Immigration Issues in the 112th Congress*, by Ruth Ellen Wasem.

[161] Prepared by Marc R. Rosenblum, Specialist in Immigration Policy, mrosenblum@crs.loc.gov, 7-7360.

Travelers seeking admission at ports of entry are required to present a travel document, typically a passport or its equivalent and (for non-U.S. citizens) either a visa authorizing permanent or temporary admission to the United States or proof of eligibility for admission through the Visa Waiver Program. Foreign nationals are subject to security-related and other background checks prior to being issued a visa or to receiving travel authorization through the Visa Waiver Program. The utility of these background checks depend fundamentally on screening at ports of entry, where CBP officers verify the authenticity of travelers' documents and that each document belongs to the person seeking admission (i.e., confirm the traveler's identity). Identity confirmation relies in part on biometric checks through the US-VISIT system (see "Entry-Exit System"), which matches travelers fingerprints against information provided during the visa application process and recorded in the State Department's Consular Consolidated Database.

The concentration of inspection activity at the border means that sufficient resources must be present in order to ensure efficient operations. Congestion at ports of entry is costly to businesses at the border and in the interior. CBP thus faces considerable pressure to provide for the rapid processing of individuals crossing the border, but expedited processing can lead to missed opportunities for interdicting threats. Moreover, investment in ports of entry has not kept pace with rapid growth in international travel and trade, and there is inadequate infrastructure to manage flows at many ports of entry. Thus, one perennial issue for Congress is how to allocate resources for port of entry infrastructure, including the maintenance and improvement of existing ports, the construction of new ports, and the number of OFO inspectors.

In an effort to streamline admissions without compromising security, CBP has implemented several trusted traveler programs. Trusted traveler programs require applicants to clear criminal and national security background checks prior to enrollment, to participate in an in-person interview, and to submit fingerprints and other biometric data. Individuals are ineligible to participate in a trusted traveler program if they are inadmissible to the United States, provide false or incomplete information on trusted traveler applications; have been convicted of a criminal offense, have outstanding warrants, or are subject to an investigation; or have been found in violation of customs, immigration, or agriculture laws. Trusted travel enrollees are re-checked against certain security databases every 24 hours, and they undergo additional screening every time they enter the United States and every time they renew their trusted traveler membership.[162] CBP currently operates four trusted traveler programs: Global Entry, which allows expedited screening of passengers arriving at 20 major U.S. airports;[163] NEXUS, which is a joint U.S.-Canadian program for land, sea, and air crossings between the United States and Canada, including through dedicated vehicle lanes at 19 land ports;[164] the Secure Electronic Network for Travelers Rapid Inspection (SENTRI), which allows expedited screening at land POEs on the U.S.-Mexican border, including through dedicated vehicle lanes at 10 land ports;[165] and the Fast and Secure Trade Program (FAST), which allows expedited screening for U.S., Mexican, and Canadian commercial truck drivers, including through dedicated truck lanes at 55 land ports on the northern and southern borders.[166]

[162] Susan Holliday, "Global Entry Takes Off," *CBP Frontline*, Winter 2011, p. 7.

[163] Ibid.

[164] U.S. Customs and Border Protection, "Fact Sheet: NEXUS," http://www.cbp.gov/linkhandler/cgov/newsroom/fact_sheets/travel/nexus_fact.ctt/nexus_fact.pdf

[165] U.S. Customs and Border Protection, "SENTRI Program Description," http://www.cbp.gov/xp/cgov/travel/trusted_traveler/sentri/sentri.xml.

[166] U.S. Customs and Border Protection, "Fact Sheet: Fast and Secure Trade," http://www.cbp.gov/linkhandler/cgov/
(continued...)

Entry-Exit System[167]

The Illegal Immigration Reform and Immigrant Responsibility Act (IIRIRA) of 1996 required the development of an automated entry-exit system that collects a record of departure for every alien departing the United States; matches exit records against alien arrival records, and allows the identification through online searches of nonimmigrants who remain beyond their period of authorized stay.[168] Subsequent legislation has revised and expanded this entry-exit requirement on several occasions.[169] Following the September 11, 2001 terrorist attacks, the tracking of nonimmigrants who overstayed their visas remained an important goal, but border security at and between ports of entry became the paramount concern.

Since 2004 DHS has also collected biometric data, including digital photographs and fingerprints, from certain travelers entering the United States through the U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) system.[170] Biometric data are added to the Automated Biometric Identification System (IDENT) database, which also includes biometric data from individuals apprehended at U.S. borders. The entry component of US-VISIT started at 115 airports and 14 sea ports beginning in January, 2004, expanded to the 50 busiest land POEs by the end of 2004, and has been operational at almost all U.S. ports of entry since December 2006.[171] In November 2007, the system upgraded its data collection from two fingerprint to ten prints, a change that increased its accuracy for identification purposes and that allows US-VISIT data to be checked against the Federal Bureau of Investigation's (FBI) Automated Fingerprint Identification System (IAFIS).[172] Since January 2009, US-VISIT has collected biometric data from all non-U.S. citizens entering the United States except for Canadian nationals admitted as visitors, U.S. lawful permanent residents (LPRs) returning from cruises that begin and end in the United States or entering at land ports of entry, Mexican nationals with border crossing cards, and travelers with

(...continued)

newsroom/fact_sheets/travel/fast/fast_fact.ctt/fast_fact.pdf.

[167] Prepared by Marc R. Rosenblum, Specialist in Immigration Policy, mrosenblum@crs.loc.gov, 7-7360.

[168] §110 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (P.L. 104-208, Division C).

[169] See CRS Report RL32234, *U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) Program*, by Lisa M. Seghetti and Stephen R. Vina.

[170] US-VISIT is a stand-alone division within DHS's National Protection and Programs Directorate.

[171] US-VISIT was operational at all 115 airports, 14 seaports, and 154 of 170 land ports. According to GAO, US-VISIT was not deployed to the remaining land POE's because most visitors subject to US-VISIT requirements were not authorized to use them or because, in two cases, the ports did not have the necessary transmission lines to operate US-VISIT. See U.S. Government Accountability Office, *Homeland Security: Key US-VISIT Components at Varying Stages of Completion, but Integrated and Reliable Schedule Needed*, GAO-10-13, November 2009, p. 7, http://www.gao.gov/new.items/d1013.pdf.

[172] IAFIS conducts criminal and terrorist background checks in response to requests from federal, state, and local law enforcement agencies by checking fingerprints against the IAFIS database of fingerprints, criminal histories, photographs, and biographic information. The IAFIS database includes the records of more than 66 million subjects in its criminal master file along with more than 25 million civil fingerprints. See Federal Bureau of Investigation, "Integrated Automated Fingerprint Identification System," http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/iafis/iafis.

other visas explicitly exempted from the program.[173] These exemptions include more than three-quarters of all nonimmigrants entering the United States.[174]

The entry-exit system is also required to record the identity of travelers who leave the United States so that DHS can identify individuals who overstay their visas and gather data that may be of value for intelligence analysis. But the exit component has proven difficult to implement. Currently, DHS uses biographic information from I-94 forms and other traveler information to match entry and exit data through the Arrival and Departure Information System (ADIS) database. ADIS included over 250 million biographic records as of July 2011;[175] but biographic matching (i.e., names, birthdates, and other identifying information) cannot confirm the identity of departing travelers. A further limitation is that while I-94 forms are routinely collected from foreign nationals exiting at air and sea ports, collection is infrequent at land ports.

Collection of *biometric* data from exiting travelers would confirm their identity by matching fingerprints against over 230 million records in IDENT,[176] but such collection has proven even more difficult. US-VISIT tested a pair of pilot programs to collect biometric data from departing air passengers in May-July 2009, but GAO concluded that the pilots provided "limited" information "toward the department's understanding of an air exit solution's operational impacts."[177] The system also tested a pilot program in 2009-2010 to collect biometric data from departing temporary workers at a pair of land ports in Arizona. Overall, a November 2009 GAO analysis concluded that "US-VISIT has not developed and employed an integrated approach to scheduling, executing, and tracking the work that needs to be accomplished to deliver [a] Comprehensive Exit solution."[178] The Administration's FY2012 budget proposes to cancel funding for biometric air exit programming, and to focus instead on entry-exit matching of biographic data based on I-94 forms. Delays in the implementation of US-VISIT's exit-tracking system have been an ongoing subject of congressional attention,[179] and Congress may continue to monitor this issue.

[173] U.S. Department of Homeland Security, Privacy Impact Assessment Update for the United States Visitor and Immigrant Status Indicator Technology Program (U.S.-VISIT) in Conjunction with the Final Rule (73 FR 7743), Enrollment of Additional Alien in US-VISIT," February 10, 2009, http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit_addl%20aliens.pdf

[174] During FY2009, CBP inspectors tallied 163 million nonimmigrant admissions to the United States. Mexican nationals with border crossing cards and Canadian nationals traveling for business or tourist purposes accounted for the vast majority of admissions to the United States in FY2009, with approximately 126.8 million entries. The remaining categories and countries of the world contributed the 36.2 million I-94 admissions in FY2009. Randall Monger and Macready Barr, *Nonimmigrant Admissions to the United States: 2009*, U.S. Department of Homeland Security Office of Immigration Statistics, Annual Flow Report, April 2010, http://www.dhs.gov/xlibrary/assets/statistics/publications/ni_fr_2009.pdf.

[175] Data provided by US-VISIT legislative affairs. August 29, 2011.

[176] Ibid.

[177] U.S. Government Accountability Office, *Homeland Security: US-VISIT Pilot Evaluations Offer Limited Understanding of Air Exit Options*, GAO-10-860, August 2010, p. 4, http://www.gao.gov/new.items/d10860.pdf.

[178] U.S. Government Accountability Office, *Homeland Security: Key US-VISIT Components at Varying Stages of Completion, but Integrated and Reliable Schedule Needed*, GAO-10-13, November 19, 2009, page 20.

[179] See e.g., Letter from Charles Schumer, U.S. Senator, to Janet Napolitano, Secretary of Homeland Security, September 23, 2009, http://schumer.senate.gov/new_website/record.cfm?id=318194.

Enforcement between Ports of Entry[180]

Between ports of entry, CBP's U.S. Border Patrol (USBP) is responsible for enforcing U.S. immigration law and other federal laws along the border and for preventing all unlawful entries into the United States, including entries of terrorists, other unlawful aliens, instruments of terrorism, narcotics, and other contraband. In the course of discharging its duties, the Border Patrol patrols 7,494 miles of U.S. international borders with Mexico and Canada and the coastal waters around Florida and Puerto Rico.[181]

Shortly after the creation of DHS, the Border Patrol was directed to formulate a new National Border Patrol Strategy that would better reflect the realities of the post 9/11 security landscape. In September 2004, the Border Patrol unveiled the current strategy, which places emphasis on interdicting terrorists and features five main objectives: establishing the substantial probability of apprehending terrorists and their weapons as they attempt to enter illegally between the ports of entry; deterring illegal entries through improved enforcement; detecting, apprehending, and deterring smugglers of humans, drugs, and other contraband; leveraging "Smart Border" technology to multiply the deterrent and enforcement effect of agents; and reducing crime in border communities, thereby improving the quality of life and economic vitality of those areas.[182] The Border Patrol's National Strategy is an attempt to lay the foundation for achieving "operational control" over the border, which the Border Patrol defines as "the ability to detect, respond, and interdict border penetrations in areas deemed as high priority for threat potential or other national security objectives."[183]

In 2005, the Department of Homeland Security announced a comprehensive multi-year plan, the Secure Border Initiative (SBI) to secure U.S. borders and reduce illegal migration, reiterating many of the themes from the 2004 National Strategy.[184] Under SBI, the Department announced plans to obtain operational control of the northern and southern borders within five years by focusing attention in five main areas: increased staffing, improved detention and removal capacity, surveillance technology, tactical infrastructure, and interior enforcement.

The concentration of personnel, surveillance technology, and infrastructure on the southwest border is designed to make it more difficult to cross the border between ports of entry and thereby to funnel traffic toward ports of entry, where inspection resources makes detection of unauthorized immigrants and illegal goods more likely. Along with enhanced detention and removal procedures, these enforcement efforts also seek to raise the costs of apprehension for unauthorized immigrants and to disrupt smuggling networks by making it more difficult for aliens to quickly reenter the United States after being apprehended.

Congress may reconsider the allocation of resources across these elements of border enforcement and/or the overall border enforcement strategy. While DHS has invested substantial resources in border security—including $3.62 billion requested for CBP's enforcement between ports of entry

[180] Prepared by Marc R. Rosenblum, Specialist in Immigration Policy, mrosenblum@crs.loc.gov, 7-7360.

[181] Also see CRS Report RL32562, *Border Security: The Role of the U.S. Border Patrol*, by Chad C. Haddal.

[182] Department of Homeland Security, Bureau of Customs and Border Protection, "National Border Patrol Strategy," September 2004. Hereafter referred to as *Border Patrol National Strategy*.

[183] *Border Patrol National Strategy*, p. 3.

[184] US Department of Homeland Security, "Fact Sheet: Secure Border Initiative," press release, November 2, 2005, http://www.dhs.gov/xnews/releases/press_release_0794.shtm.

in FY2012—the effectiveness of border enforcement is difficult to measure based on border apprehensions, which is the primary metric DHS uses to gauge enforcement outcomes. Border apprehensions fell to a 39-year low in FY2010,[185] but the drop in apprehensions may be a function of the downturn in U.S. labor markets, among other variables, in addition to more effective enforcement. Moreover, apprehensions data do not account for aliens who evade detection and successfully enter the United States. Some members of Congress also may worry about possible adverse consequences of border enforcement, including the humanitarian impact on certain immigrants, harmful effects on the environment, effects on border communities, effects on U.S. foreign relations, and the possibility that border enforcement unintentionally causes some unauthorized immigrants to remain in the United States rather than returning to their countries of origin. On the other hand, some Members of Congress have called for increased investment in border enforcement, particularly as a precursor to a broader debate about immigration reform.

Congress may also question the relative priority attached to the southwest and northern borders. While the southwest border has experienced more unauthorized immigration, some security experts have warned that the northern border may represent a more important point of vulnerability when it comes to terrorism and related threats to homeland security—especially in light of the more limited enforcement resources deployed there.[186]

CBP Integrity[187]

An additional issue of possible concern to Congress is the integrity of CBP agents and others involved with security at and between U.S. ports of entry. CBP places a great amount of responsibility upon its inspection officers, and smugglers and other nefarious actors have attempted—sometimes successfully—to infiltrate CBP. Moreover, criminals have reportedly made extensive efforts to surreptitiously enroll CBP officers on their payrolls, particularly in the wake of drug supply chain interruptions by the ongoing Mexican drug-related violence and the tactical measures implemented by DHS. To counteract such efforts, DHS has ramped up its internal investigation efforts to root out any double agents. These integrity programs have been accompanied by increased professionalization measures, such as the addition of law enforcement retirement benefits for CBP officers that incentivize employees to resist corruption. Congress appropriated $10 million in emergency supplemental funding in FY2010 to support these integrity efforts (P.L. 111-230) and continues to hold hearings on the subject.[188]

[185] DHS reported 516,992 deportable aliens located in FY2010, the lowest number since 1972; see U.S. Department of Homeland Security Office of Immigration Statistics, *Yearbook of Immigration Statistics*, Washington, DC, 2010.

[186] See e.g., U.S. Government Accountability Office, *Border Security: Enhanced DHS Oversight and Assessment of Interagency Cooridination is Needed for the Northern Border*, GAO-11-97, December 2010, http://www.gao.gov/new.items/d1197.pdf.

[187] Prepared by Marc R. Rosenblum, Specialist in Immigration Policy, mrosenblum@crs.loc.gov, 7-7360.

[188] U.S. Congress, Senate Committee on Homeland Security and Governmental Affairs, Ad Hoc Subcommittee on Disaster Recovery, *Border Corruption: Assessing Customs and Border Protection and the Department of Homeland Security Inspector General's Office Collaboration in the Fight to Prevent Corruption*, 112th Cong., 1st sess., June 9, 2011.

Disaster Preparedness, Response and Recovery

Disaster Assistance Funding[189]

The majority of disaster assistance provided by the Federal Emergency Management Agency (FEMA) to states and localities after a declared emergency or major disaster is funded with monies from the Disaster Relief Fund (DRF).[190]

In general, Congress annually appropriates budget authority to the DRF to ensure that funding is available for recovery projects from previous incidents (some of these projects take several years to complete) and to create a reserve to pay for emergencies and major disasters that might occur that fiscal year. Any remaining balance in the DRF at the end of the fiscal year is carried over to the next fiscal year. However, in some cases—particularly in recent years—there have been shortfalls in the DRF. In such cases, additional budget authority has typically been provided through a continuing resolution or an emergency supplemental appropriation.[191]

From FY2005 to FY2010, Congress provided additional budget authority for the DRF through a combination of supplemental and continuing appropriations nine times. The reliance on emergency supplemental appropriations has been of particular congressional concern. Policymakers generally view an emergency supplemental appropriation as a back-up measure to provide funding for an unexpected situation because the appropriated funds are not subject to spending caps.

While some of the emergency supplemental appropriations passed by Congress have clearly been for large, unexpected incidents such as Hurricane Katrina, it could be argued that it has become a common budgetary practice to budget the DRF at a lower level and then rely on emergency supplemental appropriations to make up the difference later in the fiscal year. For example, the average monthly DRF expenditure for disaster assistance is $350 million—or $4.2 billion dollars a year. In contrast, the average amount enacted for the DRF in a regular appropriation since FY2005 has been around $2 billion a year. It could therefore be argued that the enacted amount for the DRF does not reflect the true cost of disasters. In addition, the funds provided through emergency supplemental appropriations are not subject to spending caps—including unrelated spending. It might be argued that the budgetary practice is used as a mechanism to (1) project smaller budget deficits, and (2) evade discretionary spending caps.

In response to these concerns, Congress may consider passing reforms to reduce federal expenditures for disaster assistance, or to address their impact on the national debt. These include the use of offsets, changing emergency and major disaster declaration criteria to limit the number of events eligible for federal assistance, and reducing the standard 75% federal to state cost-share for recovery to a lower percentage (such as 50%).[192]

---

[189] Prepared by Bruce R. Lindsay, Analyst in American Government, Government and Finance Division, blindsay@crs.loc.gov, 7-3752.

[190] For further analysis on emergency and major disaster declarations see CRS Report RL34146, *FEMA's Disaster Declaration Process: A Primer*, by Francis X. McCarthy

[191] For further analysis on the DRF and emergency supplemental appropriations see CRS Report R40708, *Disaster Relief Funding and Emergency Supplemental Appropriations*, by Bruce R. Lindsay and Justin Murray.

[192] For further analysis on federal cost-shares see CRS Report R41101, *FEMA Disaster Cost-Shares: Evolution and* (continued...)

DHS State and Local Preparedness Grants[193]

State and local governments have primary responsibility for most domestic public safety functions. When facing difficult fiscal conditions, state and local governments may reduce their level of contribution towards public safety and, consequently, homeland security preparedness, due to increasing pressure to address tight budgetary constraints and fund competing priorities. Since state and local governments fund the largest percentage of public safety expenditures, this may have a significant impact on the national preparedness level. On March 30, 2011, President Obama issued a presidential policy directive that required the Secretary of DHS to develop and submit to the President a national preparedness goal within 180 days of the date of the directive. The national preparedness goal must be developed in coordination with federal, state, local, tribal, and territorial governments:

> The national preparedness goal shall be informed by the risk of specific threats and vulnerabilities – taking into account regional variations – and include concrete, measurable, and prioritized objectives to mitigate that risk. The national preparedness goal shall define the core capabilities necessary to prepare for the specific types of incidents that pose the greatest risk to the security of the Nation.[194]

This presidential policy directive supersedes a previous national preparedness homeland security directive (HSPD-8) issued after 9/11, which initiated a national preparedness goal:

> Strengthen the preparedness of the United States to prevent and respond to threatened or actual domestic terrorist attacks, major disasters, and other emergencies by requiring a national domestic all-hazards preparedness goal.[195]

Prior to 9/11, there were only three federal grant programs available to state and local governments to address homeland security: the State Domestic Preparedness Program administered by the Department of Justice, the Emergency Management Performance Grant (EMPG) administered by the Federal Emergency Management Agency (FEMA), and the Metropolitan Medical Response System (MMRS) administered by the Department of Health and Human Services. Since that time, several additional homeland security grant programs were added to ensure state and local preparedness, including the State Homeland Security Grant Program (SHSGP), Citizen Corps Program (CCP), Urban Area Security Initiative (UASI), Driver's License Security Grants Program (REAL ID), Operation Stonegarden grant program (Stonegarden), Regional Catastrophic Preparedness Grant Program (RCPG), Public Transportation Security Assistance and Rail Security Assistance grant program (Transit Grants), Port Security Grants (Port Security), Over-the-Road Bus Security Assistance (Over-the-Road), Buffer Zone Protection Program (BZPP), Interoperable Emergency Communications Grant Program (IECGP), and Emergency Operations Center Grant Program (EOC). In FY2012, the President's budget request included funding for SHSGP, CCP, UASI, Stonegarden, Transit Grants, Port Security, BZPP, and EMPG.

(...continued)

Analysis, by Francis X. McCarthy.

[193] Prepared by Natalie M. Keegan, Analyst in American Federalism and Emergency Management Policy, nkeegan@crs.loc.gov, 7-9569.

[194] Presidential Policy Directive 8, *National Preparedness*(PPD-8), issued on March 30, 2011.

[195] Homeland Security Directive 8, *National Preparedness* (HSPD-8), issued on December 17, 2003.

While state and local governments receive federal assistance for preparedness activities, this federal assistance accounts for only a small percentage of overall state and local spending for public safety. On average, total expenditures for all state and local governments for public safety is $218 billion annually.[196] Public safety expenditures include costs associated with the functions of police protection, fire protection, correction, and protective inspections and regulations.[197] In FY2010, Congress appropriated approximately $4.1 billion to federal grant programs for state and local government homeland security preparedness.[198] In FY2011, Congress appropriated approximately $3.3 billion to federal grant programs for state and local government homeland security preparedness. For FY2012, the President requested $3.8 billion in federal grants for state and local government homeland security preparedness. These amounts account for less than two percent of state and local government public safety costs. Since state and local governments are critical in the overall preparedness efforts of the nation, Congress may wish to review how to best provide assistance to ensure appropriate levels of state and local preparedness in the changing fiscal conditions facing the nation.

Firefighter Assistance Programs[199]

While firefighting activities are traditionally the responsibility of states and local communities, Congress has established federal firefighter assistance grant programs within DHS to provide additional support for local fire departments. During the 1990s shortfalls in state and local budgets, coupled with increased responsibilities of local fire departments, led many in the fire community to call for additional financial support from the federal government. In 2000, the 106th Congress established the Assistance to Firefighters Grant Program (AFG), which provides grants to local fire departments for firefighting equipment and training. In the wake of the 9/11 attacks, the scope and funding for AFG were subsequently expanded. Additionally in 2003, the 108th Congress established the Staffing for Adequate Fire and Emergency Response (SAFER) program, which provides grants to support firefighter staffing.[200]

In the 112th Congress, debate over firefighter assistance programs takes place within the appropriations and reauthorization processes. With respect to annual appropriations, arriving at funding levels for AFG and SAFER is subject to two countervailing considerations. On the one hand, the economic turndown and inadequate state and local public safety budgets have led many to argue for the necessity of maintaining federal grant support for fire departments. On the other hand, concerns over reducing overall federal discretionary spending has led others to question whether continued or reduced federal support for AFG and SAFER is warranted.

Another appropriations issue involves SAFER waivers. Congress—since FY2009—has included language in appropriations bills that waives various restrictions on SAFER grants (such as cost share requirements and a prohibition against using grant funds to rehire laid-off firefighters). The inclusion of waivers reflects concerns that modifications to the SAFER rules may be necessary to

[196] U.S. Census Bureau, *State and Local Government Finance Summary Report*, April 2011, p. 7.

[197] The definition of state and local public safety expenditures is based on the U.S Census Bureau's definition of public safety for the annual surveys of state and local government finances.

[198] This amount includes appropriations for the Firefighters Assistance Grants.

[199] Prepared by Lennard G. Kruger, Specialist in Science and Technology Policy, lkruger@crs.loc.gov, 7-7070.

[200] For more information, see CRS Report RL32341, *Assistance to Firefighters Program: Distribution of Fire Grant Funding*, by Lennard G. Kruger, and CRS Report RL33375, *Staffing for Adequate Fire and Emergency Response: The SAFER Grant Program*, by Lennard G. Kruger.

lessen the financial burden of SAFER grant recipients, thereby enabling more fire departments to participate in the program. As with AFG and SAFER funding levels, the issue is the appropriate mix of firefighting funding responsibility between states/localities and the federal government.

Meanwhile, the most recent authorization of AFG expired on September 30, 2009, while SAFER's authorization expired on September 30, 2010. In the 111th Congress, reauthorization legislation for AFG and SAFER was passed by the House, but was not passed by the Senate. In the 112th Congress, virtually identical versions of the House and Senate bills from the 111th Congress have been introduced. Debate over the AFG reauthorization has reflected a competition for funding between career/urban/suburban departments and volunteer/rural departments. Also as part of the reauthorization debate, the 112th Congress may consider whether some SAFER rules and restrictions governing the hiring grants should be permanently eliminated or altered in order to make it economically feasible for more fire departments to participate in the program.

Emergency Communications Infrastructure: Next Generation Technologies[201]

Emergency Communications is generally used to describe the process of delivering critical information before, during, and after a disaster. Congress and other policy makers typically evaluate these communications systems on three separate tracks: the emergency alert system; 911 services; and first responder communications – especially wireless networks. Although policies may be considered separately, the technologies that support emergency communications are converging toward a common platform using the Internet Protocol. IP-enabled networks will deliver the emergency communications of the future, integrating response and recovery across multiple functions of emergency management, preparedness, response, and recovery.

Increasingly, the same IP-enabled infrastructure will be used in managing communications-based systems that are vital to preventing loss of life and property. For example, the same infrastructure that supports next-generation 911 systems is available for smart grid management by utilities, transmitting information that helps to mitigate the consequences of power outages and surges. As the current emergency alert system is redeveloped to take advantage of next-generation information technologies, the same sensors used to provide information about potentially life-threatening events in evacuations will also be used for daily monitoring of traffic conditions. In addition, the new communications technologies envisioned by the public safety community and policy-makers are expected to work seamlessly with new technologies being introduced by the commercial sector. The keystone of these developments is the transition to fourth-generation (4G) wireless technologies and the supporting IP-enabled network infrastructure.

The 112th Congress has shown great concern for protecting public safety, life, and property and meeting the needs of the nation's first responders. In particular, Congress has supported development of a wireless broadband network for public safety communications. Proposed legislation and draft discussion bills in both chambers appear to be agreement on three points:

- To assure nationwide coverage, some federal governance is required to coordinate planning and deployment of the network or networks.

[201] Prepared by Linda K. Moore, Specialist in Telecommunications Policy, lmoore@crs.loc.gov.

- The capital investment and start-up operating costs are projected to be substantial.
- Access to suitable spectrum is essential for better communications support for first responders across the United States.

The bills under consideration differ – often significantly – on the how much spectrum should be allocated to public safety, the form of federal governance, and the source of needed funds. Efforts continue in both chambers to find an effective compromise.[202]

National Preparedness System[203]

Since the formation of the Federal Emergency Management Agency (FEMA), the all-hazards approach to emergency management[204] has given rise to a sophisticated system of intergovernmental relationships. In response to the terrorist attacks of September 11th 2001, President Bush signed a series of homeland security presidential directives aimed at improving interagency coordination as well as the comprehensive emergency management system of 1) preparedness, 2) mitigation, 3) response, and 4) recovery.

On March 30 2011, President Obama updated Homeland Security Directive -8 (HSPD-8), which provided federal guidance on homeland security and emergency management preparedness, with Presidential Policy Directive-8 (PPD-8). Compared to HSPD-8, PPD-8 increases emphasis on national preparedness, building and sustaining key emergency management capabilities, and using metrics and assessments to gauge preparedness levels. Like HSPD-8, and in compliance with Section 641 of the Post-Katrina Emergency Management and Reform Act (hereafter the Post-Katrina Act),[205] PPD-8 calls for the development of a national preparedness goal and a national preparedness system.

The preparedness goal and system in PPD-8 requires the adoption of a series of frameworks including a National Prevention Framework, a National Protection Framework, a National Mitigation Framework, a National Response Framework (NRF), and a National Disaster Recovery Framework. Currently, only the NRF has been approved and put into use—the National Disaster Recovery Framework is still in draft form but expected to be implemented in the near future. The status of the other frameworks is unclear.

The establishment of a national preparedness system may be of congressional concern for a variety of reasons. Critics might argue that prevention and protection are related and requiring two frameworks for the same purpose would be duplicative or redundant. In addition, it might also be argued that fragmenting emergency management activities into a system of frameworks could confuse or hinder interagency coordination. Others may question why the frameworks are

[202] Additional information is available in CRS Report R41842, *Funding Emergency Communications: Technology and Policy Considerations*, by Linda K. Moore.

[203] Prepared by Bruce R. Lindsay and Francis X. McCarthy, Government and Finance Division.

[204] The all-hazards approach to emergency management is based on the assumption that there are common sets of preparedness and response procedures and practices applicable to any type of event and an economy of scale is achieved by planning and preparing for incidents in generic terms rather than preparing and responding to specific threats and hazards.

[205] P.L. 109-295, 120 Stat. 1394-1463.

being developed concurrently with a national preparedness goal, if the frameworks are based on the goal.

Public Health and Medical Services[206]

The nation's public health emergency management laws expanded considerably in the past decade, reflecting lessons from the airliner and anthrax attacks of 2001 and Hurricane Katrina, in particular. More recently the H1N1 influenza pandemic, Haiti earthquake, *Deepwater Horizon* incident, and nuclear plant failures following an earthquake and tsunami in Japan each revealed persistent challenges in the nation's readiness for public health and medical emergencies. Among the gaps that were spotlighted: existing response plans may not sufficiently anticipate situations that arise; the technology needed to assess threats (such as radiation or chemical exposure) may be limited; medical countermeasures (i.e., vaccines, antidotes, or treatments for harmful exposures) may not be available in adequate amounts, if at all; the means to distribute existing countermeasures in a timely manner may be limited; the medical system may lack sufficient capacity to provide care in response to a mass casualty incident; and funding for response costs may not be immediately available, if at all. Given the robust roles of the private sector and state and local governments, as well as a churning workforce in preparedness and response efforts, the ability of the federal government to affect these efforts through funding and other policies may also be limited.

The 109th Congress passed the Pandemic and All-Hazards Preparedness Act (PAHPA, P.L. 109-417)[207] and several other laws that established, reorganized, or reauthorized public health and medical preparedness and response activities in the Departments of Health and Human Services (HHS) and Homeland Security (DHS). The authorizations of appropriations for a number of provisions in these laws have expired, or are due to expire at the end of FY2011. The 112th Congress is proceeding with reauthorization of these laws, focused in particular on improving federal programs to assure the availability of countermeasures.[208]

Funding for incident response is a challenge when an incident does not lead to a declaration under the Stafford Act.[209] The HHS Secretary has authority for a no-year Public Health Emergency Fund, but Congress has not appropriated monies to the fund for many years.[210] Assistance under the Stafford Act can help federal, state, and local agencies with the costs of public health activities such as assuring food and water safety, and monitoring illness rates in affected communities. However, there is no federal assistance program designed purposefully to cover the uninsured or uncompensated costs of individual health care (including mental health care) that

[206] Prepared by Sarah A. Lister, Specialist in Public Health and Epidemiology, slister@crs.loc.gov, 7-7320. For more information, see CRS Report R41646, *Public Health and Medical Emergency Management: Issues in the 112th Congress*, by Sarah A. Lister, and CRS Report R41123, *Federal Efforts to Address the Threat of Bioterrorism: Selected Issues and Options for Congress*, by Frank Gottron and Dana A. Shea.

[207] CRS Report RL33589, *The Pandemic and All-Hazards Preparedness Act (P.L. 109-417): Provisions and Changes to Preexisting Law*, by Sarah A. Lister and Frank Gottron.

[208] CRS Report RL33907, *Project BioShield: Appropriations, Acquisitions, and Policy Implementation Issues for Congress*, by Frank Gottron.

[209] CRS Report RL34724, *Would an Influenza Pandemic Qualify as a Major Disaster Under the Stafford Act?*, by Edward C. Liu, and CRS Report R41234, *Potential Stafford Act Declarations for the Gulf Coast Oil Spill: Issues for Congress*, by Francis X. McCarthy.

[210] CRS Report RL33579, *The Public Health and Medical Response to Disasters: Federal Authority and Funding*, by Sarah A. Lister.

may be needed as a consequence of a disaster. There is not consensus that this should be a federal responsibility. Nonetheless, if faced with a mass casualty incident, hospitals, physicians, and other providers could face considerable pressure to deliver care without a clear source of reimbursement.[211] On several occasions, Congress has provided special assistance to address emergency-related health care costs after an incident.[212]

FEMA Disaster Assistance Recoupment[213]

The Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act) authorizes the President to issue "major disaster" or "emergency" declarations before or after catastrophes occur.[214] Emergency declarations trigger aid that protects property, public health, and safety and lessens or averts the threat of an incident becoming a catastrophic event. A major disaster declaration, issued after catastrophes occur, constitutes broader authority for federal agencies to provide supplemental assistance to help state and local governments, families and individuals, and certain nonprofit organizations recover from the incident. The assistance for families and individuals is clustered under the rubric that the Federal Emergency Management Agency (FEMA) designates as Individual Assistance.

Individual Assistance (IA) includes various forms of help for families and individuals following a disaster event. The assistance authorized by the Stafford Act can include housing assistance, disaster unemployment assistance, crisis counseling and other programs intended to address the needs of people. The most prominent form of IA is the Individuals and Households Program (IHP) that can provide direct financial assistance to disaster victims.

Since Hurricane Katrina in 2005, FEMA has distributed more than $7 billion in IHP payments.[215] In 2010, the Department of Homeland Security (DHS) Office of Inspector General identified 160,000 potentially improperly awarded IHP payments totaling $643 million of those payments.[216] Improper payments are payments that were made in error or overpayments pursuant to statutory, regulatory, or administrative provisions. Improper payments for IHP may include payments made to ineligible individuals, duplicate payments to the same household, and payments for items or expenses covered by the individuals insurance company or another federal agency. In some cases, the improper payment or overpayment was made based upon information provided by the individual when they applied for federal disaster assistance that was later found

[211] Depending on its implementation, the recently enacted health care law (the Patient Protection and Affordable Care Act, PPACA, P.L. 111-148, as amended) may mitigate this concern by decreasing the ranks of the uninsured. However, PPACA does not address ongoing debate about the use of worker's compensation to cover the costs of chronic health conditions that arise after a work-related exposure, and that may or may not have been caused by that exposure.

[212] CRS Report RL33927, *Selected Federal Compensation Programs for Physical Injury or Death*, coordinated by Sarah A. Lister and C. Stephen Redhead; GAO, *Hurricane Katrina: Allocation and Use of $2 Billion for Medicaid and Other Health Care Needs*, GAO-07-67, February 28, 2007, http://www.gao.gov; CRS Report R40554, *The 2009 Influenza Pandemic: An Overview*, by Sarah A. Lister and C. Stephen Redhead; and CRS Report R41232, *FY2010 Supplemental for Wars, Disaster Assistance, Haiti Relief, and Other Programs*, coordinated by Amy Belasco.

[213] Prepared by Francis X. McCarthy, Analyst in Emergency Management Policy, fmccarthy@crs.loc.gov, 7-9533.

[214] 42 U.S.C. 5721 et seq.

[215] Testimony of Matt Jadacki, Assistant Inspector General for Emergency Management Oversight, U.S. Department of Homeland Security, before the U.S. Senate, Homeland Security and Governmental Affairs Committee, Ad Hoc Subcommittee on Disaster Recovery and Intergovernmental Affairs, *Preventing Improperly Paid Federal Assistance in the Aftermath of Disasters,* Mar. 17, 2011, p. 2.

[216] Ibid.

to be incorrect when FEMA reviewed the file. For example, some applicants gave the address of vacant lots and cemeteries as the damaged property address. While some of the recoupment may be a result of an individuals effort to defraud the federal government, the majority of the 160,000 payments were not attributed to fraud.[217] Most fraud cases are turned over to the Inspector General's office for investigation.

The largest portion of potential improper payments was made under disaster declarations for hurricanes Katrina and Rita, with $621.6 million in IHP payments. Approximately $21.7 million in payments have been made during subsequent disaster declarations. FEMA began recouping improper IHP payments in March 2011 and are recouping payments made under recent disasters and working back to payments made for the Hurricane Katrina in 2005.[218]

Congress may wish to consider how such recoupments are carried out and how Section 312 of the Stafford Act that prohibits duplication of benefits with other federal programs, is executed under the current recoupment process.[219] In addition, Congress may also consider the relationship of the National Flood Insurance Program to federal disaster assistance, particularly Section 408 home repair assistance and how that relationship informs recoupment decisions.

DHS Management and Administration

The Management Budget[220]

Title I of the Homeland Security Appropriations bill contains the funding for the primary management functions of the Department of Homeland Security. Originally envisioned as a skeleton staff, the headquarters and management functions have grown in response to criticism of the Department's ability to effectively oversee its own activities. In debates over departmental funding, questioning the size and effectiveness of the Department's management cadre is a common theme.

In FY2003, the first year of DHS operations, $195 million was provided for management accounts. In FY2011, those accounts were funded at $839 million. This growth is due to several factors, including increases in staff size required to perform oversight functions, rising personnel costs, technology investments, and increasing real estate expenses for the department's headquarters offices. In recent years, these accounts have been requested at artificially high levels due to significant capital initiatives, such as headquarters consolidation and data center migration, and personnel initiatives aimed at boosting the department's cadre of acquisition oversight staff and reducing the number of contractors in sensitive positions.

[217] U.S. Department of Homeland Security, Federal Emergency Management Agency, *Follow-up Questions and Answers: Recoupment of Disaster Assistance*, March 2011, p. 3.

[218] Testimony of Matt Jadacki, Assistant Inspector General for Emergency Management Oversight, U.S. Department of Homeland Security, before the U.S. Senate, Homeland Security and Governmental Affairs Committee, Ad Hoc Subcommittee on Disaster Recovery and Intergovernmental Affairs, *Preventing Improperly Paid Federal Assistance in the Aftermath of Disasters,* Mar. 17, 2011, p. 3.

[219] 42 U.S.C. 5155.

[220] Prepared by William L. Painter, Analyst in Emergency Management and Homeland Security Policy, wpainter@crs.loc.gov, 7-3335.

The House and Senate Appropriations Committees recommended funding the management accounts for FY2012 at $674 million and $692 million, respectively. The Administration had already expressed concern about the House funding levels prior to floor action, noting that "the funding provided in the bill for the Office of the Secretary and Executive Management would result in a reduction-in-force."[221] Despite that warning, House amendments reduced the funding in the bill by nearly $332 million from the committee's recommendation.

DHS Financial Management Reforms[222]

From its inception, DHS has faced financial management challenges. Transferring components and their budgets between agencies is a complex process in the best of situations, but doing it in the process of establishing a new department that is performing important national security missions from its first day of operations adds additional complexity. This was further compounded by inherited financial management problems that existed at several major components, including the Coast Guard, FEMA and ICE.

The department tried to develop its own financial management system in-house through a project known as "eMerge2," but failed. A second attempt was made to implement a department-wide system through contracting with outside developers under the Transformation and Systems Consolidation initiative, or TASC. After GAO ruled that DHS had improperly awarded the initial $450 million contract—the latest result from a series of protests and legal challenges that had delayed the project—the award was cancelled and the project shelved.

Although the department has been on the GAO High Risk List since it was created, progress has been made on reducing the number of material weaknesses in the department's financial controls. According to recent testimony by Deputy Chief Financial Officer Peggy Sherry, the department inherited 30 significant deficiencies in its financial systems, including 18 material weaknesses across the entire enterprise. As of May 2011, she testified that are now only six material weaknesses, and problems that stand in the way of receiving an opinion on the Department's consolidated balance sheet for FY2011 are limited to the Coast Guard.[223]

Congress will likely continue its interest in DHS's efforts to improve its internal financial systems, given the relative size of the department's budget and the current drive for stricter budgetary oversight.

Headquarters Consolidation[224]

The Department of Homeland Security's headquarters footprint occupies more than 7 million square feet of office space in about 45 separate locations in the greater Washington, DC area. This

[221] Office of Management and Budget, *Statement of Administration Policy*, H.R. 2017—Department of Homeland Security Appropriations Act 2012, Washington, DC, May 31, 2011, p. 2, http://www.whitehouse.gov/.

[222] Prepared by William L. Painter, Analyst in Emergency Management and Homeland Security Policy, wpainter@crs.loc.gov, 7-3335.

[223] U.S. Congress, House Committee on Oversight and Government Reform, Subcommittee on Government Organization, Efficiency, and Financial Management, *Department of Homeland Security Financial Management*, 112th Cong., 2nd sess., May 13, 2011.

[224] Prepared by William L. Painter, Analyst in Emergency Management and Homeland Security Policy, wpainter@crs.loc.gov, 7-3335.

is largely a legacy of how the department was assembled in a short period of time from 22 separate federal agencies who were themselves spread across the National Capital region. The fragmentation of headquarters is cited by the Department as a major contributor to inefficiencies, including time lost shuttling staff between headquarters elements; additional security, real estate, and administrative costs; and reduced cohesion among the components that make up the department.

To unify the department's headquarters functions, the department approved a $3.4 billion master plan to create a new DHS headquarters on the grounds of St Elizabeths in Anacostia. According to GSA, this is the largest federal office construction since the Pentagon was built during World War II. $1.4 billion of this project was to be funded through the DHS budget, and $2 billion through the GSA.[225] Thus far $375 million has been appropriated to DHS for the project and $871 million to GSA. Phase 1A of the project – a new Coast Guard headquarters facility – is nearing completion with the funding already provided by Congress.

The Administration requested $215 million for headquarters consolidation through the DHS budget, including $160 million for new construction at St. Elizabeths. They also requested $217 million through GSA for the project, including funding for a planned highway alterations to provide better motor vehicle access to the campus. The House provided no funding for either request in FY2012, while the Senate provided $56 million in their version of the DHS appropriations bill to complete the Coast Guard headquarters facility.[226] The Senate also included in their bill a requirement that DHS provide within 60 days of enactment an expenditure plan and an initial analysis of the mix of offices to be housed at the headquarters complex.

With headquarters consolidation remaining a priority for the Administration, appropriated funds dwindling for the project, and current budgetary constraints altering both the growth projections that were the basis for DHS's consolidation plans and the prospects for funding in coming fiscal years, legislative action in the 112th Congress will help clarify the future for this project—through reaffirmation of the original plan or changes to its schedule, scope, or scale that could be required by the level of funding for the coming year.

DHS Reorganization Authority[227]

From the establishment of the Department of Homeland Security (DHS) in January 2003 through 2007, the President and the Secretary of Homeland Security used provisions of the Homeland Security Act of 2002, most notably Section 872,[228] to implement a number of major and minor departmental reorganizations. Some reorganization activities under these authorities were carried out in conjunction with the implementation of the Post-Katrina Emergency Management Reform Act of 2006.[229]

---

[225] U.S. Congress, House Committee on Appropriations, Subcommittee on Homeland Security, *Homeland Security Headquarters Facilities*, 111th Cong., 2nd sess., March 25, 2010 (Washington: GPO, 2010), pp. 335-366.

[226] As of this writing, the Senate has not filed its version of the Financial Services Appropriations bill, which would include GSA's share of the funding.

[227] Prepared by Henry B. Hogue, Analyst in American National Government, hhogue@crs.loc.gov, 7-0642.

[228] P.L. 107-296; 116 Stat. 2135 at 2243.

[229] Implementation of certain provisions of the Post-Katrina Emergency Management Reform Act of 2006 was interwoven into a January 2007 reorganization under the Secretary's authority.

Since May 2007, Congress has limited the use of appropriated funds for carrying out Section 872 reorganizations. Section 3501 of the U.S. Troop Readiness, Veterans' Care, Katrina Recovery, and Iraq Accountability Appropriations Act, 2007, enacted on May 25, 2007, instituted such limitations for the balance of FY2007, stating:

> None of the funds provided in this Act, or P.L. 109-295 [Department of Homeland Security Appropriations Act, 2007], shall be available to carry out section 872 of P.L. 107-296 [Homeland Security Act of 2002]. [230]

Succeeding DHS appropriations acts up through and including that for FY2010 have included similar provisions.[231] The final continuing resolution for FY2011 appears to carry the FY2010 provision forward for the fiscal year ending September 30, 2011.[232]

The scope and effect of this limitation were the subject of a July 2008 Government Accountability Office (GAO) opinion.[233] This opinion raised the question of whether a reorganization could be undertaken under authorities that, absent Section 872, might be available to the Secretary. These include the authorities identified by the department: implied authority to organize and manage the department;[234] redelegation authority; and authority under 5 U.S.C. § 301, which authorizes an agency head to "prescribe regulations for the government of his department, the conduct of its employees, the distribution and performance of its business, and the custody, use, and preservation of its records, papers, and property."

Since the appropriations acts are annual, the decision of whether or not to carry over the limitation arises each year. More broadly, the question of whether and how Section 872 might be amended may be at issue as part of a reauthorization process. Such decisions might hinge, in part, on a congressional determination of the impact of Section 872 and the appropriation limitation on the management and functioning of the department.

[230] P.L. 110-28; 121 Stat. 112 at 143.

[231] See, for example, a provision of the Consolidated Appropriations Act, 2008: "None of the funds provided in this Act shall be available to carry out section 872 of Public Law 107–296." (P.L. 110-161, § 546; 121 Stat. 2080). Similar provisions were included in the Consolidated Security, Disaster Assistance, and Continuing Appropriations Act, 2009 (P.L. 110-329, § 529; 122 Stat. 3686); and the Department of Homeland Security Appropriations Act, 2010 (P.L. 111-83, § 525; 123 Stat. 2173).

[232] See P.L. 112-10, The Department of Defense and Full-Year Continuing Appropriations Act, 2011; 125 Stat. 38. Section 1104 of the act provides that, "Except as otherwise expressly provided in this division, the requirements, authorities, conditions, limitations, and other provisions of the appropriations Acts referred to in section 1101(a) shall continue in effect through the date specified in section 1106 [September 30,2011]." 125 Stat. 103. The Department of Homeland Security Appropriations Act, 2010 (P.L. 111-83), which contains the limitation provision, is among those referred to in section 1101(a).

[233] U.S. Government Accountability Office, *Department of Homeland Security—Transfer of Support Function for Principal Federal Officials*, B-316533, July 31, 2008, http://www.gao.gov/decisions/appro/316533.pdf. Hereafter, B-316533.

[234] See Basil J. Mezines, Jacob A. Stein, and Jules Gruff, *Administrative Law*, vol. 1 (New York: Matthew Bender, 2006), pp. 4-18 to 4-27.

Department of Homeland Security Personnel Issues[235]

Human resources management (HRM) has been an important consideration underlying the mission and performance of the Department of Homeland Security (DHS) since its creation. Responsibility for HRM is vested in the Office of the Chief Human Capital Officer (OCHCO), an entity organizationally and for appropriations purposes located within the Undersecretary for Management. The OCHCO is expected to play a critical role in supporting and enabling the department's Workforce Strategy for Fiscal Years 2011-2016. The current CHCO announced his retirement effective on August 3, 2011, and a new chief has been named. The CHCO position has also been changed from a political appointment to a career appointment. Issues that relate to HRM for which Congress may conduct oversight during the second session of the 112th Congress include workforce planning, leadership development and training, and human resources information technology.

Workforce Planning

Two goals included in the DHS Workforce Strategy are "[r]ecruiting a highly qualified and diverse workforce" and "[r]etaining an engaged workforce."[236] A four-day summit convened in May 2011 discussed strategic workforce planning for the department and focused on such issues as a framework and tools for planning, identifying strategic and core mission critical occupations and key workforce planning indicators to be tracked and reported, and methods to be used to measure employee competencies. A prototype that will be used to report to the Secretary on emerging trends in, and the characteristics of, the DHS workforce is being developed. The draft prototype includes such indicators as projected staffing needs, progress made against hiring goals, attrition rates, and selected DHS results from the Office of Personnel Management's annual employee viewpoint survey. With regard to measuring employee competencies, 'a competency model library' that will be available to the DHS Workforce Planning Council via a SharePoint site is under development.

Leadership Development and Training

Another goal under the department's Workforce Strategy is "[b]uilding an effective, mission-focused, diverse and inspiring cadre of leaders." The DHS congressional justification for FY2012 states that the OCHCO will develop "a comprehensive proposal" that will "identify executive resource requirements for FY2012 and FY2013." Additionally, a formal mentoring program and a rotation program, both across DHS components and government-wide, is being established to enhance and sustain the institutional knowledge of executives, managers, and supervisors and develop their leadership skills in core areas of management and administration. A succession plan for Senior Executive Service positions will also be prepared. The justification also states that the "OCHCO will design and deliver comprehensive leadership and workforce training programs for

[235] Prepared by Barbara L. Schwemle, Analyst in American National Government, bschwemle@crs.loc.gov, 7-8655. For information on other personnel issues at DHS, see CRS Reports CRS Report R40642, *Homeland Security Department: FY2010 Appropriations*, coordinated by Jennifer E. Lake and CRS Report R41189, *Homeland Security Department: FY2011 Appropriations*, coordinated by Jennifer E. Lake and William L. Painter and CRS Memorandum, *Possible Homeland Security Issues for the 112th Congress*, September 13, 2010, pp. 9-10. For a discussion of the department's balanced workforce strategy, see the section of this report authored by L. Elaine Halchin.

[236] All text in quotations in this section is from U.S. Department of Homeland Security, *Departmental Management and Operations, Under Secretary for Management, Fiscal Year 2012 Congressional Justification*, pp. 3, 10, and 12.

all personnel." Any gaps in employee competencies that are critical to the DHS mission, including skills in foreign languages, labor management, and preparedness, will continue to be identified and addressed by remedial actions. Legislation introduced, but not enacted, in the 110th Congress to authorize the department (S. 3623) included a provision that would have created an Office of the Chief Learning Officer (CLO) for DHS.[237] The CLO's responsibilities would have included establishing and managing the implementation of a learning and development strategy for the department, coordinating with DHS components about training and education activities at the component level, and creating courses or programs. Congress may reconsider this approach as part of an overall review of how DHS coordinates and manages the development of its employees.

Human Resources Information Technology (HRIT)

HRIT is an account under the OCHCO appropriation. A long-term strategic plan for HRIT is being redefined and implemented by the CHCO, the Chief Information Officer, and other department officials. DHS operates four enterprise solutions related to human resources (HR): National Finance Center Corporate for payroll and personnel, EmpowHR for personnel, webTA for time and attendance, and the eOPF for electronic personnel folders. The department's congressional justification notes, however, "the critical need for enterprise solutions" for "staffing, learning management, performance management, and personnel accountability for continued operation, in the event of a declared emergency." Increased efficiencies in the delivery of HR services across the department is a goal underlying the strategy.

HRM at DHS will likely continue to be an issue for oversight by Congress. Suggestions for regular review and evaluation of the OCHCO have been previously mentioned.[238] To further inform Congress about the relationship between the department's workforce planning policies and processes, DHS could be directed to include, in its annual congressional justification, or as an electronic file on its website, an easily understood crosswalk table that illustrates how those plans, in both the short- and long-term, coordinate with the Quadrennial Homeland Security Review and the overall national security strategy. A goal of the Workforce Strategy is "[s]olidifying a unified DHS culture of mission performance, adaptability, accountability, and results." Several initiatives to foster "One DHS," including the completion of a comprehensive Correspondence and Style Guidance Handbook, are currently underway. Congress may choose to specifically review, on an annual basis, the mechanisms for, and operation of, collaboration and coordination within the department as part of its consideration of the DHS budget submission.

Acquisition[239]

The Department of Homeland Security ranked seventh in procurement spending in FY2010, but it experienced the largest growth among major federal agencies for the period FY2002 to FY2010. In constant dollars (FY2010), DHS spent $1.1 billion in FY2002 and $13.6 billion in FY2010.[240]

[237] The Government Accountability Office and the Department of Commerce, for example, have Chief Learning Officer positions.

[238] CRS Memorandum, Possible Homeland Security Issues for the 112th Congress, September 13, 2010, p. 9.

[239] Prepared by L. Elaine Halchin, Specialist in American National Government, ehalchin@crs.loc.gov, 7-0646.

[240] Using data obtained from USASpending.gov, CRS calculated FY2010 constant dollars.

Organization of the Acquisition Function

Approximately 22 executive branch organizations were pulled together to form the Department of Homeland Security. To some extent, the structure of procurement operations within DHS is a legacy of how the department was created. The following eight DHS components have their own contracting activities: Customs and Border Protection (CBP); Federal Emergency Management Agency (FEMA); Federal Law Enforcement Training Center (FLETC); Immigration and Customs Enforcement (ICE); Office of the Chief Procurement Officer (OCPO), which has two contracting activities;[241] Transportation Security Administration (TSA); U.S. Coast Guard (USCG); and U.S. Secret Service.[242] Some observers have questioned whether this structure, where responsibility is shared by the chief procurement officer and the other components, is optimal. For example, the Government Accountability Office (GAO) has noted that the department's acquisition function "creates ambiguity about who is accountable for acquisition decisions because it depends on a system of dual accountability and cooperation and collaboration between the CPO and the component heads."[243]

Acquisition Workforce

As the Services Acquisition Reform Act (SARA) Panel noted in its 2007 report, the federal acquisition workforce has "shortcomings in terms of size, skills, and experience...."[244] and DHS is no exception. GAO has reported that the department does not have "adequate staff to effectively plan and execute contracts."[245] In the same report, GAO acknowledged that "DHS's initiatives are positive steps toward building an effective acquisition workforce," but also noted that the department needs to engage in long-term strategic workforce planning.[246] In an effort to address its acquisition workforce needs, the department's FY2012 budget request included $24.2 million for an acquisition workforce initiative. The House Committee on Appropriations declined to provide funding for the initiative, stating that the information it has received from DHS was "insufficient to enable the Committee to understand the basis for the proposed increase...."[247]

Balanced Workforce Initiative

In early 2009, DHS announced that, as part of its efficiency review, department components would examine how to achieve a proper balance between federal employees and contractor

[241] The Office of the Chief Procurement Officer has two contracting offices, the Office of Procurement Operations and the Office of Selective Acquisitions.

[242] U.S. Department of Homeland Security, Office of Inspector General, *Update on DHS' Procurement and Program Management Operations*, OIG-11-91, June 2011, p. 4, at http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_11-91_Jun11.pdf.

[243] U.S. Government Accountability Office, *Department of Homeland Security: Progress and Continuing Concerns with Acquisition Management*, GAO-08-1164T, September 17, 2008, p. 4, http://www.gao.gov/new.items/d081164t.pdf.

[244] U.S. Government Accountability Office, Department of Homeland Security: A Strategic Approach Is Needed to Better Ensure the Acquisition Workforce Can Meet Mission Needs, GAO-09-30, November 19, 2008, p. 5, at http://www.gao.gov/new.items/d0930.pdf.

[245] Ibid., p. 2.

[246] Ibid., pp. 27-28.

[247] U.S. Congress, House Committee on Appropriations, *Department of Homeland Security Appropriations Bill, 2012*, 112th Cong., 1st sess., May 26, 2011, H.Rept. 112-91 (Washington: GPO, 2011), p. 15.

employees. Achieving the proper balance generally involves determining which agency functions, if any, are to be reserved for federal employee performance. For example, only federal employees are to perform inherently governmental functions.[248] Approximately one year later, this particular effort had been renamed the balanced workforce initiative. The initiative involves "ensur[ing] that no inherently governmental functions are performed by contractors ... put[ting] in place rigorous review procedures to ensure that future contract actions do not increase our [the department's] reliance on contractors; and ... coordinating workforce assessments across the Department to seek economies and service improvements and reduce our reliance on contractors."[249] To aid department personnel in determining whether a function should be reserved for performance by federal employees, DHS has developed an instrument known as the balanced workforce strategy tool (or survey).

The topics discussed here suggest several questions that may be of interest to the 112th Congress. Regarding the structure of DHS' acquisition function, has the department satisfactorily addressed concerns about its system of dual accountability? Has the department considered other options for organizing its acquisition function? Turning to the department's acquisition workforce, what are the possible consequences of being unable to fund its acquisition workforce initiative in FY2012? What acquisition tasks, or activities, are most likely to be affected by the lack of a fully staffed and trained acquisition workforce? Under its balanced workforce initiative, has DHS discovered contractor employees performing inherently governmental functions? Has the department identified any situations where it had ceded control over its mission and operations to contractor employees? How many contractors, and which contracts, might be affected by the agency's efforts to achieve a balanced workforce?

Consolidated Terrorist Watch Lists[250]

Prior to the 9/11 attacks, terrorist watch lists were maintained by several agencies primarily to prevent foreign terrorists from entering the United States. In September 2003, under the Homeland Security Presidential Initiative 6 (HSPD-6),[251] the U.S. government's use of watch lists was consolidated and expanded to better screen such persons at consular offices and international ports of entry, and to better track them if they manage to enter the United States.[252] While the post-9/11 terrorist screening policies have resulted in valid watch list matches, misidentifications have also been a recurring issue for Congress.[253] Initially, such problems were most frequently associated with the Transportation Security Administration (TSA), but misidentifications have also emerged as a problem for the U.S. Customs and Border Protection (CBP).[254] In December

[248] 48 C.F.R. §7.503(a).

[249] U.S. Department of Homeland Security, *FY2011 Budget in Brief*, p. , at http://www.dhs.gov/xlibrary/assets/budget_bib_fy2011.pdf.

[250] Prepared by William J. Krouse, Specialist in Domestic Security and Crime Policy, wkrouse@crs.loc.gov, 7-2225.

[251] Homeland Security Presidential Directive 6 (HSPD-6), *Integration and Use of Screening Information* (Sept. 16, 2003), http://www.dhs.gov/xabout/laws/gc_1214594853475.shtm.

[252] HSPD-6, *Integration and Use of Screening Information* (Sept. 16, 2003), http://www.dhs.gov/xabout/laws/gc_1214594853475.shtm.

[253] See CRS Report RL33645, *Terrorist Watchlist Checks and Air Passenger Prescreening*, by William J. Krouse and Bart Elias.

[254] See, e.g., Rahman v. Chertoff, No. 05-C 3761, 2010 U.S. Dist. LEXIS 31634 (N.D. Ill. Mar. 31, 2010). Initially, this case was a class action law suit where the plaintiffs asserted that, as a result of watch lists maintained by the Department of Homeland Security, their constitutional rights are being violated as they experience lengthy stops, (continued...)

2010, however, TSA fully implemented its Secure Flight program and the frequency of terrorist watch list misidentifications is expected to abate. In addition, the Department of Homeland Security (DHS) has established a "Watchlist Service," which is a mirror database of the Federal Bureau of Investigation (FBI) consolidated database of terrorist watch list records. While this move brings the U.S. government closer to the goal of employing a single, consolidated terrorist watch list, it arguably further diffuses responsibility for terrorist watch list records under an arrangement that could have already been justifiably described as Byzantine.

Under HSPD-6, the terrorist identification and watch list functions previously performed by State's Bureau of Intelligence and Research (INR) were split between the Terrorist Threat Integration Center (TTIC), later renamed the National Counterterrorism Center (NCTC),[255] and the then newly established Terrorist Screening Center (TSC). The NCTC is responsible for indentifying international terrorists and collating all available information on those persons in the Terrorist Identities Datamart Environment (TIDE).[256] Federal agencies within the U.S. Intelligence Community[257] forward nominations to the NCTC to include known and suspected international terrorists into TIDE based upon both foreign and criminal intelligence. The FBI, on the other hand, is responsible for identifying both international and domestic terrorists (in the latter case, based upon criminal intelligence).[258] The FBI-administered TSC is responsible for maintaining the consolidated Terrorist Screening Database (TSDB), into which both international and domestic watch list records are consolidated. The TSC tailors watch list records to meet the missions of frontline screening agencies and downloads them from the TSDB into their screening systems. Consequently, these watch lists are in most cases only subsets of the TSDB. In addition, the TSC has developed comprehensive procedures for handling encounters with known and suspected terrorists and their supporters, and provides terrorist screening agencies with around-the-clock operational support in the event of possible terrorist encounters.

(...continued)

questioning, and detention upon reentry to the United States. While the suit is ongoing, the class was recently decertified. *See* Rahman v. Chertoff, 530 F.3d 622 (7th Cir. 2008).

[255] Pursuant to the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458), TTIC was renamed the National Counterterrorism Center (NCTC) and was charged with serving as the central hub for the fusion and analysis of information collected from all foreign and domestic sources on international terrorist threats. The NCTC was placed under the aegis of the Director of National Intelligence (DNI).

[256] According to the FBI, international terrorists include those persons who carry out terrorist activities *under foreign direction*. For this purpose, they may include both citizens and noncitizens, while citizens are included under the rationale that citizens could be recruited by foreign terrorist groups. Or, noncitizens (aliens) could immigrate to the United States and naturalize (become citizens), having been unidentified terrorists before entry, or having been recruited as terrorists sometime after their entry into the United States.

[257] The Intelligence Community includes the Central Intelligence Agency (CIA); the National Security Agency (NSA); the Defense Intelligence Agency (DIA); the National Geospatial-Intelligence Agency (GIA); the National Reconnaissance Office (NRO); the other DOD offices that specialize in national intelligence through reconnaissance programs; the intelligence components of the Army, Navy, Air Force, and Marine Corps, the FBI, the Department of Energy, and the Coast Guard; the INR at the DOS, the Office of Intelligence and Analysis at Department of the Treasury, and elements of the DHS that are concerned with the analyses of foreign intelligence information (50 U.S.C. §401a(4)).

[258] Domestic terrorists *are not under foreign direction*, and operate entirely within the United States. According to the Administration, both sets of data (on international and domestic terrorists) include, when appropriate, information on "United States persons." The definition of "United States person" is found at 50 U.S.C. §1801(i): a citizen of the United States, an alien lawfully admitted for permanent residence (as defined §1101(a)(2) of Title 8), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation that is incorporated in the United States, but does not include a corporation or an association that is a foreign power, as defined in subsection (a)(1), (2), or (3) of this section.

By providing tailored watch list records from the TSDB, the TSC supports the terrorist screening activities of the DHS's TSA and CBP, as well as the Department of State's Bureau of Consular Affairs (CA). Similar terrorist watch list records are also shared with the Department of Defense and selected foreign governments. As of May 2010, the TSDB contained information on 422,674 individuals, who are known or suspected of being international or domestic terrorists.[259] Due to aliases and name variants, however, the TSDB included over 1.7 million records related to watch-listed individuals.[260]

Under HSPD-6, the TSC Director is responsible for developing policies and procedures related to the criteria for including terrorist identities data in the consolidated TSDB and for measures to be taken in regard to misidentifications, erroneous entries, outdated data, and privacy concerns. However, the TSC does not collect intelligence, and has no authority to do so. In fact, all intelligence or data entered into the TSDB are actually collected by other agencies with the U.S. Intelligence Community in accordance with applicable, pre-existing authorities. As a consequence, the TSC is limited in its ability to address certain issues related to misidentifications because it is restricted from divulging classified or law enforcement-sensitive information to the public under certain circumstances. DHS, as well as its frontline screening agencies (such as TSA and CBP), arguably confronts the same limitation, because many terrorist watch list records, while possibly declassified, are based on classified intelligence collected by other agencies. Such records would probably be considered security sensitive information.

Despite these limitations, Congress required the TSA and DHS to establish appeals procedures.[261] Under these requirements, persons who are identified as terrorism-related security threats based on records in the TSDB would have the ability to appeal such determinations and have such records, if warranted, modified to alleviate such occurrences in the future.[262] Congress also required DHS to establish an Office of Appeals and Redress where individuals, who believe they have been delayed or prohibited from boarding a commercial aircraft because they were wrongly identified as a threat, would have a timely and fair process for redress.[263] To meet these requirements, DHS established the Traveler Redress Inquiry Program (TRIP) as a mechanism for addressing watch list misidentification issues and other situations where passengers feel that they have been unfairly or incorrectly delayed or denied boarding or identified for additional security screening at airport screening checkpoints, ports of entry or border checkpoints, or when seeking to access other modes of transportation. Nevertheless, many civil libertarians and privacy advocates do not view either the TSC or DHS as being in a position under current law to provide adequate and timely redress to persons misidentified as terrorists or improperly watch-listed as terrorists.[264]

In July 2010, the transmission of terrorist watch list records from the FBI/TSC to DHS/TSA was reengineered, when a "secure" system-to-system arrangement was established that allows the

[259] Federal Bureau of Investigation, Office of Congressional Affairs.

[260] Ibid.

[261] P.L. 108-458, Section 4012(a)(1)(G) (2004).

[262] Ibid.

[263] Implementing Recommendations of the 9/11 Commission Act of 2007, P.L. 110-53, Section 1606 (2007).

[264] See Paul Rosenzweig and Jeff Jonas, *Correcting False Positives: Redress and the Watch List Conundrum*, Heritage Foundation, Legal Memorandum, no. 17 (June 17,2005), 13 pp.; and Constitution Project, *Promoting Accuracy and Fairness in the Use of Government Watch Lists*, (December 2006), 49 pp.

entire contents of the TSDB to be made available to DHS on a "near real-time" basis.[265] At DHS, this mirror database is known as the "Watchlist Service (WLS)."[266] In July 2011, DHS proposed exempting its WLS from the Privacy Act of 1974 in the same way that the FBI did the TSDB,[267] a move that caused privacy advocates to renew calls for a more transparent and robust terrorist watch list redress process and to question again the U.S. government's expanded use of terrorist watch list records under HSPD-6.[268]

Homeland Security Research and Development[269]

Many stakeholders have identified advances in research and development (R&D) as key to creating new or improved technologies that defend against homeland security threats. R&D is generally a multi-year endeavor with significant risk of failure. Additionally, it may take years to realize any benefits from R&D investments. The Administration and Congress have differing visions regarding performance of R&D in DHS. In both FY2011 and FY2012, DHS requested to consolidate its R&D activities. Congress denied the DHS request in FY2011 and is considering the FY2012 request. In addition, some congressional and stakeholder expectations regarding the effectiveness and efficiency of agency performance have not been met. The 112th Congress may continue to focus attention on whether investments in homeland security research and development net appropriate rewards, how the distribution of investments among homeland security topics and between research and development activities leads to a balanced portfolio, and what the appropriate funding level for DHS R&D is during a time of fiscal constraint.

The DHS homeland security R&D activities have substantial scope, as these activities must attempt to meet the needs of both DHS component agencies and other customers outside of the agency, such as first responders. Stakeholders continue to debate the optimal approach to maximizing DHS R&D effectiveness. Some advocates call for substantial increases in particular areas of research and development, citing that a dedicated research effort with significant investments as more likely to yield technology breakthroughs. Some stakeholders call for a rebalancing of the investment portfolio with an increased focus on technology development, arguing that many prototypes under development in the private sector need only a small boost to convert them to procurable technologies. Other stakeholders call for a rebalancing of the investment portfolio towards long-term research activities, warning that DHS will lack research outcomes to develop into prototypes if long-term research languishes. Finally, portions of the stakeholder community suggest using a high-risk, high-reward investment strategy similar to that undertaken by the Defense Advanced Research Projects Agency (DARPA) so as to make "leap-ahead" advances relative to terrorist capabilities.

The DHS is not the sole federal funder of homeland security R&D, but the DHS Under Secretary for Science and Technology (S&T) is responsible for coordinating homeland security R&D

[265] U.S. Department of Homeland Security, *Privacy Impact Assessment Update for the Watchlist Service*, July 14, 2010, p. 1.

[266] Ibid.

[267] Department of Homeland Security, Privacy Office, "Privacy Act of 1974: Implementation of Exemptions; Department of Homeland Security/All—030 Use of the Terrorist Screening Database Records," 76 *Federal Register* 39315, July 6, 2011.

[268] Charles S. Clark, "Privacy Groups Challenge Proposal Expanding Access to Terrorist Watch List," *Government Executive*, August 15, 2011.

[269] Prepared by Dana A. Shea, Specialist in Science and Technology Policy, dshea@crs.loc.gov, 7-6844.

activities across the federal government. The DHS Under Secretary for S&T has experienced challenges in attempting to coordinate these activities and has failed to develop a federal homeland security R&D strategy. Congress has historically been interested in identifying and overcoming the barriers to such coordination. The 112th Congress may conduct oversight of how any new strategic approaches taken by DHS address these longstanding concerns, set milestones for future performance, and project meeting the needs of DHS components and the first-responder community.

For FY2011 and FY2012, DHS requested that Congress transfer some research and development activities within the purview of the Domestic Nuclear Detection Office to the S&T Directorate. Additionally, DHS Under Secretary for S&T O'Toole has reprioritized and consolidated ongoing research and development activities within the S&T Directorate. The results of the proposed transfer and current reprioritization and consolidation might change the productivity of DHS R&D activities, which have been criticized by stakeholders as having little to show for the federal investment. Congress did not approve this transfer in FY2011, and the House-passed DHS appropriations bill for FY2012 also does not approve this transfer. In addition, the House-passed DHS appropriations bill would reduce appropriations for R&D in the S&T Directorate by 42% relative to FY2011. This may indicate that the slow rate of return shown by S&T Directorate R&D investments is not acceptable to some congressional policymakers.

Author Contact Information

William L. Painter, Coordinator
Analyst in Emergency Management and Homeland Security Policy
wpainter@crs.loc.gov, 7-3335

Jerome P. Bjelopera
Specialist in Organized Crime and Terrorism
jbjelopera@crs.loc.gov, 7-0622

Jared T. Brown
Analyst in Emergency Management and Homeland Security Policy
jbrown@crs.loc.gov, 7-4918

Claudia Copeland
Specialist in Resources and Environmental Policy
ccopeland@crs.loc.gov, 7-7227

Bart Elias
Specialist in Aviation Policy
belias@crs.loc.gov, 7-7771

Kristin M. Finklea
Analyst in Domestic Security
kfinklea@crs.loc.gov, 7-6259

John Frittelli
Specialist in Transportation Policy
jfrittelli@crs.loc.gov, 7-7033

Frank Gottron
Specialist in Science and Technology Policy
fgottron@crs.loc.gov, 7-5854

L. Elaine Halchin
Specialist in American National Government
ehalchin@crs.loc.gov, 7-0646

Henry B. Hogue
Analyst in American National Government
hhogue@crs.loc.gov, 7-0642

Natalie Keegan
Analyst in American Federalism and Emergency Management Policy
nkeegan@crs.loc.gov, 7-9569

William J. Krouse
Specialist in Domestic Security and Crime Policy
wkrouse@crs.loc.gov, 7-2225

Lennard G. Kruger
Specialist in Science and Technology Policy
lkruger@crs.loc.gov, 7-7070

Sarah A. Lister
Specialist in Public Health and Epidemiology
slister@crs.loc.gov, 7-7320

Francis X. McCarthy
Analyst in Emergency Management Policy
fmccarthy@crs.loc.gov, 7-9533

Linda K. Moore
Specialist in Telecommunications Policy
lmoore@crs.loc.gov, 7-5853

John D. Moteff
Specialist in Science and Technology Policy
jmoteff@crs.loc.gov, 7-1435

Paul W. Parfomak
Specialist in Energy and Infrastructure Policy
pparfomak@crs.loc.gov, 7-0030

David Randall Peterman
Analyst in Transportation Policy
dpeterman@crs.loc.gov, 7-3267

R. Eric Petersen
Specialist in American National Government
epetersen@crs.loc.gov, 7-0643

Shawn Reese
Analyst in Emergency Management and Homeland Security Policy
sreese@crs.loc.gov, 7-0635

John Rollins
Specialist in Terrorism and National Security
jrollins@crs.loc.gov, 7-5529

Marc R. Rosenblum
Specialist in Immigration Policy
mrosenblum@crs.loc.gov, 7-7360

Barbara L. Schwemle
Analyst in American National Government
bschwemle@crs.loc.gov, 7-8655

Dana A. Shea
Specialist in Science and Technology Policy
dshea@crs.loc.gov, 7-6844

Lorraine H. Tong
Analyst in American National Government
ltong@crs.loc.gov, 7-5846

Bruce R. Lindsay
Analyst in American National Goverment
blindsay@crs.loc.gov, 7-3752