POLICY ESSAY

A LEGISLATIVE PRESCRIPTION FOR CONFRONTING 21ST-CENTURY RISKS TO THE HOMELAND

REPRESENTATIVE BENNIE G. THOMPSON*

I. INTRODUCTION

In the wake of the terrorist attacks of September 11, 2001, President George W. Bush addressed a joint session of Congress and announced the creation of a Cabinet-level Office of Homeland Security.[1] Just a few months later, Congress enacted the Homeland Security Act of 2002, mandating the creation of the U.S. Department of Homeland Security ("DHS" or "the Department") and setting in motion the largest reorganization of the federal government since World War II.[2] That same year, the House of Representatives established the Select Committee on Homeland Security ("CHS" or "the Committee") to oversee the new department.[3]

Over the last eight years, DHS and Congress have worked to strengthen the security of the United States. Congress has enacted legislation to address security gaps and conducted vigorous oversight over DHS. However, notwithstanding legislative and oversight successes, several additional measures must be adopted to create a more robust, comprehensive, and long-lasting framework to improve our nation's homeland security.

This Essay evaluates the success of past homeland security policies and offers proposals for the future. In Part II, this Essay highlights what should be four broad underlying principles of all future policies: policy-making free from fear, technological advancement, empowering the citizenry, and consolidating congressional jurisdiction. In Parts III, IV, and V, respectively, the Essay turns to specific problems and proposals in the areas of critical infrastructure protection, disaster preparedness and response, and border security. Taken together, these proposals focus on identifying and strengthening areas most vulnerable to attack, encouraging more effective collaboration between

---

* Member, House of Representatives (D-Miss.). Representative Thompson has served as Chairman of the Committee on Homeland Security since the beginning of the 110th Congress. For assisting him in the authoring of this Essay, he would like to acknowledge the contributions of Alison Northrop, Stephen Viña, and Michael Beland, each of whom is Subcommittee Director.

[1] Address Before a Joint Session of the Congress on the United States Response to the Terrorist Attacks of September 11, 2 PUB. PAPERS 1140 (Sept. 20, 2001).

[2] Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135 (codified as amended in scattered sections of 6 U.S.C.).

[3] H.R. Res. 449, 107th Cong. (2002).

DHS and private parties, updating technology, and avoiding jurisdictional hurdles by consolidating jurisdiction over DHS in one congressional committee. Perhaps most importantly, the proposals argue for a more effective collaboration between government and citizens so that citizens' desire to help protect the nation can be put to good use.

II. The Fundamental Principles of Homeland Security in the 21st Century

In fulfilling its mandate to create a "secure America, a confident public, and a strong and resilient society and economy,"[4] DHS should focus on three things: moving away from the "politics of fear," leveraging 21st-century technology, and providing our society with notions of empowerment and resilience. Perhaps most importantly, congressional jurisdiction for DHS must be better streamlined to promote stronger oversight and efficiency at the Department.

A. Delivering Freedom from Fear

The "politics of fear" is a concept with a storied past. This concept refers to "decision makers' promotion and use of audience beliefs and assumptions about danger, risk, and fear in order to achieve certain goals."[5] Elected officials often use this tactic to convince the public that opposing those officials' policies would make the world a more dangerous place, thus providing a political justification for executing controversial or sensitive actions.[6] This mentality was evident in some of the drastic measures taken by the federal government immediately after September 11. For example, the Department of Justice and, later, DHS, pursued thousands of foreigners under the guise of immigration enforcement in the hopes of capturing terrorists, thereby blurring the distinction between antiterrorism and immigration enforcement.[7] One of the more notorious programs included the special registration and fingerprinting of nonimmigrant aliens from countries of special interest, including Iran, Iraq, Libya, Sudan, and Syria.[8] Furthermore, even though there was no evidence that terrorists had attempted to cross our

---

[4] DHS, One Team, One Mission, Securing Our Homeland 3 (2008), *available at* http://www.dhs.gov/xlibrary/assets/DHS_StratPlan_FINAL_spread.pdf [hereinafter DHS, One Team, One Mission].

[5] David L. Altheide, Terrorism and the Politics of Fear 15 (2006).

[6] *See* Jim VandeHei & Howard Kurtz, *The Politics of Fear, Kerry Adopts Bush Strategy of Stressing Dangers*, Wash. Post, Sept. 29, 2004, at A1 (citing commercials from President Bush and Senator John Kerry (D-Mass.) during the presidential campaign of 2004, President Jimmy Carter's portrayal of President Ronald Reagan as a warmonger in 1980, and President Lyndon Johnson's "daisy girl" ad that warned of nuclear war if Senator Barry M. Goldwater (R-Ariz.) was elected in 1964).

[7] Edward Alden, The Closing of the American Border 90, 98 (2008).

[8] *See* 8 C.F.R. § 264.1 (2009).

southwestern border surreptitiously,[9] that possibility was partially used to justify the construction of hundreds of miles of border fencing.[10] Former Homeland Security Secretary Tom Ridge even admitted to being pressured by the White House to raise the terror alert level to influence the 2004 presidential election.[11]

If the vision of DHS is truly to create a "secure America"[12] and a "confident public,"[13] DHS cannot create policies grounded in fear. Instead, it must develop well-considered policies that reflect rational analysis of a situation, and it must present these proposals to the public in a reasonable, non-panic-inducing manner.

B. Harnessing the Power of Technology

The increasingly globalized world is becoming more reliant on technology. Potential adversaries and criminal networks use sophisticated technology to maintain a competitive advantage and, in some cases, to conduct nefarious activities. The Federal Bureau of Investigation has identified multiple cyber threats to America's critical infrastructure information networks, including threats from foreign nations, domestic criminals, and hackers.[14] Yet, DHS and its federal partners continue to struggle to keep pace technologically with the rest of the world and, more alarmingly, with terrorists and criminal networks. Along our borders, for example, DHS has spent over one billion dollars on its most recent "virtual fence" initiative but has yet to

---

[9] *Current and Projected National Security Threats to the United States: Hearing Before the S. Select Comm. on Intelligence*, 109th Cong. 40–41 (2005) [hereinafter *National Security Threats Hearing*] (statement of Admiral James Loy, Deputy Secretary, DHS) (stating that while al-Qaida officials were considering entering the United States through its southwestern border, there was no conclusive evidence that they had done so).

[10] *See id.* (stating that "[r]ecent information from ongoing investigations, detentions, and emerging threat streams strongly suggests that al-Qaida has considered using the Southwest Border to infiltrate the United States" and claiming that "[s]everal al-Qaida leaders believe operatives can pay their way into the country through Mexico and also believe illegal entry is more advantageous than legal entry for operational security reasons"); *see also* Dave Montgomery, *Rice, in Mexico, Calls for Stronger Borders*, ST. PAUL PIONEER PRESS, Mar. 11, 2005, at A7 ("Secretary of State Condoleezza Rice said . . . that al-Qaida terrorists may be trying to sneak into the United States through Mexico and Canada and promised a 'robust' effort to strengthen border security.").

[11] TOM RIDGE, THE TEST OF OUR TIMES: AMERICA UNDER SIEGE. . . AND HOW WE CAN BE SAFE AGAIN 235–39 (2009).

[12] DHS, ONE TEAM, ONE MISSION, *supra* note 4, at 3.

[13] *Id.*

[14] U.S. Gov't Accountability Office, GAO-08-526, Information Security: TVA Needs to Address Weaknesses in Control Systems and Networks 8 (2008); *see also* Jeff Bliss, *Chinese Hackers Attack U.S. Computers, Thompson Says*, BLOOMBERG.COM, Feb. 12, 2009, http://www.bloomberg.com/apps/news?pid=20601089&sid=aT4zhjs27ldQ&refer=china ("Chinese government and freelance hackers are the primary culprits behind as many as several hundred daily attacks against U.S. government, electric-utility and financial computer networks, a senior congressman said.").

receive a truly effective product.[15] Instead, DHS has reallocated resources to expedite construction of a traditional border wall.[16]

Advanced technology must be a central priority for the federal government generally, and for DHS in particular. Moreover, as the government looks at advanced security technologies, it must integrate innovative ideas from all of America, including ideas from small and minority-owned businesses.

C. Strengthening the Citizenry

After September 11 and Hurricane Katrina, the nation witnessed the power of community. By the thousands, first responders and volunteers from all over the country, undeterred by danger, responded to the calls for service.[17] One of the main goals of DHS should be to draw upon the desire and ability of the citizenry to help in a time of crisis and to channel that energy into securing the homeland.

This goal has been difficult to meet. Upon releasing the updated National Strategy for Homeland Security in 2007, President Bush announced that "[t]o best protect the American people, homeland security must be a responsibility shared across our entire Nation."[18] However, incorporating the viewpoints and concerns of state, local, tribal, and private sectors has often proved challenging. For example, with respect to the construction of border fencing in Texas by DHS, CHS routinely heard landowners complain about abuses of power and lack of consultation.[19]

---

[15] *See generally* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-09-896, SECURE BORDER INITIATIVE: TECHNOLOGY DEPLOYMENT DELAYS PERSIST AND THE IMPACT OF BORDER FENCING HAS NOT BEEN ASSESSED (2009) [hereinafter GAO, SECURE BORDER INITIATIVE: DELAYS].

[16] *See* Gary Martin, *$400 Million Reallocated to Construct Border Fence*, SAN ANTONIO EXPRESS-NEWS, Sept. 23, 2008, at 4A.

[17] *See* Fred Bruning et al., *3 Months After; The Volunteers; "We Are Rejuvinated* [sic] *By Your Selfless Acts"*, NEWSDAY, Dec. 11, 2001, at W23 (noting that following September 11, tens of thousands of volunteers mobilized to aid relief efforts); Jeb Bush, *Think Locally on Relief*, TAMPA TRIB., Oct. 2, 2005, at 4 ("Within hours of Katrina's landfall, Florida began deploying more than 3,700 first responders to Mississippi and Louisiana. Hundreds of Florida National Guardsman, law enforcement officers, medical professionals and emergency managers remain on the ground in affected areas.").

[18] HOMELAND SEC. COUNCIL, EXECUTIVE OFFICE OF THE PRESIDENT OF THE U.S., NATIONAL STRATEGY FOR HOMELAND SECURITY (2007) [hereinafter NATIONAL STRATEGY FOR HOMELAND SECURITY], *available at* http://www.dhs.gov/xlibrary/assets/nat_strat_homelandsecurity_2007.pdf.

[19] *See, e.g.*, Melissa del Bosque, *Holes in the Wall: Homeland Security Won't Say Why the Border Wall is Bypassing the Wealthy and Politically Connected*, TEX. OBSERVER, Feb. 22, 2008, http://www.texasobserver.org/archives/item/15288-2688-holes-in-the-wall ("Garza points to a field across the street where a segment of the proposed 18-foot high border wall would abruptly end after passing through his brick home and a small, yellow house he gave his son. 'All that land over there is owned by the Hunts [neighbors with ties to the Bush Administration].' . . . The wall doesn't go there."); *see also* J. GAINES WILSON ET AL., THE WORKING GROUP ON HUMAN RIGHTS & THE BORDER WALL, OBSTRUCTING HUMAN RIGHTS: THE TEXAS-MEXICO BORDER WALL pt. IV (2008), *available at* http://www.utexas.edu/law/academics/centers/humanrights/borderwall/analysis/briefing-FULL-SET-OF-REPORTS.pdf (noting that

Engaging citizens to participate in homeland security matters will create a more informed and better prepared America, thereby enhancing vigilance and facilitating expedient recovery in times of tragedy.[20] When a community is better prepared, it is more likely to be resilient—capable of quickly regaining strength in the wake of disruption.[21]

D. Streamlining Homeland Security Jurisdiction

After the attacks of September 11, Congress quickly merged twenty-two disparate agencies to form DHS.[22] The 9/11 Commission—a congressionally mandated panel constituted to investigate the September 11 terrorist attacks[23]—issued a clear recommendation with respect to congressional oversight of homeland security matters: "Congress should create a single, principal point of oversight and review for homeland security."[24] General

---

"gaps" where the border fence did not cross private property occurred in high income areas of Cameron County, Texas); *Tell Me More: Expansive Border Fence Stirs Fights Over Land* (National Public Radio broadcast Mar. 3, 2008) (Professor Eloisa Tamez of the University of Texas and Mayor Pat Ahumada of Brownsville, Texas noting that they had attempted to speak with DHS regarding complaints about the border fence, but that "they have turned their deaf ears towards us").

[20] *See* CITIZEN CORPS, A GUIDE FOR LOCAL OFFICIALS, at 5–6, *available at* http://www.vdem.state.va.us/citcorps/volunteers/docs/guide_local_officials.pdf ("[T]here are many tasks that a well-trained and organized group of volunteers could perform . . . so that [first responders] could focus more on immediate emergency response needs. . . .").

[21] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-10-193, EMERGENCY PREPAREDNESS: FEMA FACES CHALLENGES INTEGRATING COMMUNITY PREPAREDNESS PROGRAMS INTO ITS STRATEGIC APPROACH 7 (2010) ("[R]esilience . . . [is] an approach that centers on investments that make a system better able to absorb the impact of an event without losing the capacity to function."); *see also* 6 U.S.C. § 317(c)(2)(I) (Supp. II 2007) (requiring DHS to coordinate with the private sector to help foster "private sector preparedness" for natural disasters, acts of terrorism, and other disasters); Citizen and Community Preparedness Act of 2008, H.R. 5890, 110th Cong. (2008); *Partnering with the Private Sector to Secure Critical Infrastructure: Has the Department of Homeland Security Abandoned the Resilience-Based Approach?: Hearing Before the Subcomm. on Transp. Sec. and Infrastructure Protection of the H. Comm. on Homeland Sec.*, 110th Cong. 3 (2008) [hereinafter *Partnering Hearing*] (statement of Sheila Jackson Lee, Member, CHS) ("A strategy based upon resilience is not a silver bullet, but it does support the critical infrastructure security objective."); *The Resilient Homeland—Broadening the Homeland Security Strategy: Hearing Before the H. Comm. on Homeland Sec.*, 110th Cong. 1 (2008) [hereinafter *Resilient Hearing*] (statement of Rep. Thompson, Chairman, CHS) ("[R]esilience is a practice which will allow a quick return to effective, if not 100 percent normal, operations in the wake of an attack or disaster.").

[22] *See* Homeland Security Act of 2002, Pub. L. No. 107-296, tit. I, §§ 101–03, 116 Stat. 2135, 2142–45 (codified as amended at 6 U.S.C. §§ 111–13 (2006, Supp. I 2007 & Supp. II 2008)); *see also* Raphael Perl, *The Department of Homeland Security: Background and Challenges*, in NAT'L RESEARCH COUNCIL OF THE NAT'L ACADS., TERRORISM: REDUCING VULNERABILITIES AND IMPROVING RESPONSES 176, 177 (2004); DHS, History: Who Became Part of the Department?, http://www.dhs.gov/xabout/history/editorial_0133.shtm (last visited May 10, 2010) (listing the twenty-two agencies that became part of DHS in 2003).

[23] *See* NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., THE 9/11 COMMISSION REPORT 361–428 (2004) [hereinafter 9/11 COMMISSION REPORT].

[24] *Id.* at 421; see also Sarah Laskow, *Is Congress Failing on Homeland Security Oversight? Despite Calls for Consolidation, Over 80 Hill Panels Still Have a Say*, CTR. FOR PUB. INTEGRITY, July 15, 2009, http://www.publicintegrity.org/articles/entry/1549 (noting that

congressional oversight of DHS was loosely consolidated into what today are CHS in the House of Representatives and the Homeland Security and Governmental Affairs Committee in the Senate.[25]

Yet this general oversight power has not prevented the fragmentation of oversight among different committees—a fragmentation that has hampered the effectiveness of the Department. Despite the creation of two primary committees of jurisdiction, nearly ninety-five other committees or subcommittees exercised jurisdiction over DHS in the 110th Congress, resulting in nearly four hundred hearings.[26] One study indicates that these numbers are an "anomaly" and highly "unusual" when compared to the number of committees and subcommittees calling for hearings from the Departments of Defense, Energy, and Transportation.[27]

This fragmentation of oversight is "tremendously debilitating" to the Department.[28] Senior DHS officials find themselves spending exorbitant amounts of time and resources preparing for numerous, often redundant, hearings and briefings—a distraction from the execution of their security mission.[29] With so many committees asserting jurisdiction, it is also difficult for Congress to provide unified guidance on the homeland security mission, thereby potentially producing less rigorous oversight.[30] DHS officials may also be subjected to retribution for siding with one committee over another.[31] This fragmented oversight of DHS has created a "tremendous imbalance

---

"[t]he recommendation that made it into the final report—the call for 'a single, principal point of oversight'—required little debate").

[25] *See* H.R. Res. 449, 107th Cong. (2002); H.R. REP. NO. 107-517 (2002); *see also* CLERK OF THE HOUSE OF REPRESENTATIVES, 111TH CONG., RULES OF THE HOUSE OF REPRESENTATIVES 6–16 R. X (2009), *available at* http://www.rules.house.gov/ruleprec/111th.pdf [hereinafter HOUSE RULES] (enumerating House committees and their legislative jurisdictions); CHS, Homeland Security Committee Overview, http://homeland.house.gov/about/index.asp (last visited Apr. 12, 2010) (noting that the House Homeland Security Committee was "first formed as a Select, non-permanent Committee").

[26] Timothy Balunis, Jr. & William Hemphill, *Escaping the Entanglement: Reversing Jurisdictional Fragmentation over the Department of Homeland Security*, 6 J. HOMELAND SEC. & EMERGENCY MGMT. art. 58, at 1–2 (2009).

[27] *Id.* at 6.

[28] MICHAEL L. KOEMPEL, CONG. RESEARCH SERV., HOMELAND SECURITY: COMPENDIUM OF RECOMMENDATIONS RELEVANT TO HOUSE COMMITTEE ORGANIZATION AND ANALYSIS OF CONSIDERATIONS FOR THE HOUSE, AND 109TH AND 110TH CONGRESSES EPILOGUE 12 (2007) (quoting David King).

[29] *See The President's Fiscal Year 2009 Budget Request for the Department of Homeland Security: Hearing Before the H. Comm. on Homeland Sec.*, 110th Cong. 3–5 (2008) (statement of Peter T. King, Ranking Member, CHS); Balunis & Hemphill, *supra* note 26, at 2; Laskow, *supra* note 24.

[30] *See* Laskow, *supra* note 24 ("When you have oversight conducted by numerous committees and subcommittees you tend not to get the rigor you need in oversight." (quoting Lee Hamilton, Vice Chair, 9/11 Comm'n)).

[31] *See* KOEMPEL, *supra* note 28, at 54 ("Thus, it will wind up that some committees . . . will say to that Department of Homeland Security, unless you do X . . . we are going to take it out on the department. And you will have fragmentation that will be pulling the department apart." (quoting James Schlesinger, Former Sec'y, Dep't of Energy)).

between the executive branch and the legislative branch," and, in the words of congressional scholar David King, "Congress must catch up."[32]

House oversight over DHS should be consolidated into one committee to minimize bureaucratic red tape, increase accountability, and provide better security. While a department as new and diverse as DHS certainly needs strong congressional oversight, it is too much for the Department to have almost two hundred percent more oversight than the aforementioned departments combined.[33]

Moreover, CHS should be the body with primary jurisdictional authority over DHS, given both its purpose and its record of success in overseeing the Department. Despite the complex web of committees with jurisdictional interests in DHS, CHS successfully moved an authorization bill for DHS through the House of Representatives[34] and navigated the jurisdictional interests of ten different committees to pass the historic 9/11 Act in the 110th Congress.[35] In the 111th Congress, CHS worked with three other committees of jurisdiction to pass landmark chemical facility security legislation.[36] This consolidation of oversight responsibility over DHS is necessary for the Department to function more effectively.

III. Critical Infrastructure Protection: History, Problems, and Proposals

September 11 demonstrated to Americans that the nature of warfare had changed. Terrorists recognize that they cannot mount an effective attack by an army or a navy on one of our borders. Instead, they attack where masses of people gather and where commercial transactions are channeled, thus leveraging comparatively scarce resources to cause maximum fear and thereby hoping to prompt political concessions.[37]

---

[32] *Id.* at 12 (quoting David King).

[33] *See* Balunis & Hemphill, *supra* note 26, at 1.

[34] *See* Department of Homeland Security Authorization Act for Fiscal Year 2008, H.R. 1684, 109th Cong. (2007).

[35] *See* Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, 121 Stat. 266 (codified as amended in scattered sections of 6 U.S.C.).

[36] *See* Chemical Facility Anti-Terrorism Act of 2009, H.R. 2868, 111th Cong. (as passed by House of Representatives, Nov. 6, 2009). The U.S. House of Representatives passed H.R. 2868 by a vote of 230-193. 155 Cong. Rec. H12,534 (daily ed. Nov. 6, 2009) (Roll Call Vote 875).

[37] Osama bin Laden has said that his goal in attacking the United States is to bring down the U.S. economy. John Mintz, *Bin Laden Lauds Costs Of War to U.S.: Recent Videotape Boasts of Inflicting Economic Damage*, Wash. Post, Nov. 2, 2004, at A2; *see also Resilient Hearing*, *supra* note 21, at 2 (statement of Rep. Thompson, Chairman, CHS) ("Simply put, the longer our economic sector is down, the more terrorists will brag that they are successful."). In addition to the September 11 attacks, the Madrid bombings in 2004, the attacks on the London Underground in 2005, and the attacks on the hotel and train station in Mumbai in 2008 all suggest a desire to attack locations that symbolize the economic strength of capitalistic and pluralistic societies.

The attacks of September 11 therefore made evident the need to secure assets and systems that previously had not been given enough security attention. Yet, precisely because of the importance of these assets and systems to the American economy and way of life, devising an effective security strategy is particularly difficult in this area. Securing every type of facility in America would have unacceptable consequences for the U.S. economy and way of life, thus delivering a partial victory to America's enemies. Instead, America needs to create a nuanced strategy that addresses significant security threats while preserving a free and open society.

This Part provides a brief history of critical infrastructure protection policy efforts and highlights some problematic areas. It then offers policy prescriptions for the future.

A. The Definition of Critical Infrastructure

The settled definition of "critical infrastructure" was established in the PATRIOT Act, which was signed into law in October 2001.[38] The Critical Infrastructures Protection Act of 2001, part of the PATRIOT Act, describes "critical infrastructure" as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[39] Critical infrastructure includes infrastructure related to our banking and finance system, our water supply, our food supply, and the transportation of goods and people. A "system" or an "asset" is not defined in the statute, thus giving the Executive Branch significant discretion.

The statutory definition of "critical infrastructure" affects infrastructure protection policy because it determines which assets and systems the government will attempt to secure. The definition attempts to strike a balance: to not be so vague as to include any infrastructure in the United States (such as a short bridge connecting two small islands of no strategic value), nor so rigid that, as new risks develop or evolve, the definition would become an obstacle to security efforts.[40]

---

[38] Pub. L. No. 107-56, 115 Stat. 272 (2001) (codified as amended in scattered titles of U.S.C.).

[39] 42 U.S.C. § 5195c(e) (2006).

[40] The federal government has recognized the necessity of maintaining this balance. While the statutory definition of "critical infrastructure" continues to evolve, the application of this definition is more selective. *See* JOHN MOTEFF & PAUL PARFOMAK, CONG. RESEARCH SERV., CRITICAL INFRASTRUCTURE AND KEY ASSETS: DEFINITION AND IDENTIFICATION 11 (2004), http://www.fas.org/sgp/crs/RL32631.pdf (citing Homeland Security Act of 2002, Pub. L. No. 107-296, §201(d)(3), 116 Stat. 2135, 2146 (codified as amended at 6 U.S.C. § 121(d)(3) (Supp. I 2007)) (requiring DHS to "identify priorities for protective and support measures by the Department"); OFFICE OF HOMELAND SECURITY, NATIONAL STRATEGY FOR HOMELAND SECURITY 30 (2002), http://www.dhs.gov/xlibrary/assets/nat_strat_hls.pdf (noting that critical infrastructure systems are "not equally important" and that "the federal government will apply a consistent methodology to focus its efforts on the highest priorities")).

There is some consensus that the PATRIOT Act's limitation of critical infrastructure to systems and assets "so vital to the United States that . . . incapacity or destruction . . . would have a debilitating impact" is too narrow, since there are in fact few, if any, assets or systems that meet this requirement.[41] For example, facilities critical to a region—while not of national significance *per se*—should be included in any definition of critical infrastructure. Accordingly, in the 9/11 Act of 2007, Congress effectively amended this definition, requiring DHS to keep a database of assets and systems that the "Secretary determines would, if destroyed or disrupted, cause national *or regional* catastrophic effects."[42]

B. The History of Critical Infrastructure Protection Policy

National security policy aims to enhance protection of the nation's critical infrastructure. Presidential Decision Directive 63 ("PDD-63"), signed by President William J. Clinton on May 22, 1998, set as a national goal the ability to protect the nation's critical infrastructure from intentional attacks, both physical and cyber, by 2000.[43] According to PDD-63, any interruptions in the ability of certain infrastructure to provide goods and services must be "brief, infrequent, manageable, geographically isolated, and minimally detrimental to the welfare of the United States."[44]

PDD-63 identified twelve sectors with critical infrastructure requiring protection: information and communications; banking and finance; water; transportation; emergency law enforcement; emergency fire services; emergency medicine; electric power, gas, and oil; law enforcement and internal security; intelligence; foreign affairs; and national defense.[45] Under PDD-63, a "lead agency"[46] was assigned to each sector. Each lead agency was directed to appoint a "Sector Liaison Official"[47] who would interact with appropriate private sector organizations—such as trade associations—and

---

[41] *See, e.g.*, *Partnering Hearing*, *supra* note 21; *Protecting the Mass Transit Critical Infrastructure in New York City and in the Nation: Hearing Before the Subcomm. on Transp. Sec. and Infrastructure Protection of the H. Comm. on Homeland Sec.*, 110th Cong. (2008); *Partnerships in Securing Critical Infrastructure: Hearing Before the Subcomm. on Transp. Sec. and Infrastructure Protection of the H. Comm. on Homeland Sec.*, 110th Cong. (2008); *The Impact of Foreign Ownership and Foreign Investment on the Security of Our Nation's Critical Infrastructure: Hearing Before the Subcomm. on Transp. Sec. and Infrastructure Protection of the H. Comm. on Homeland Sec.*, 110th Cong. (2007).

[42] Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, tit. X, § 1001, sec. 210E(a)(2), 121 Stat. 266, 372 (codified at 6 U.S.C. § 124l(a)(2) (Supp. II 2007)) ("National Asset Database") (emphasis added).

[43] The White Paper on Critical Infrastructure Protection PDD 63, 1998 WL 263839 (May 22, 1998) [hereinafter PDD–63].

[44] *Id.*; *see also* JOHN D. MOTEFF, CONG. RESEARCH SERV., CRITICAL INFRASTRUCTURES: BACKGROUND, POLICY, AND IMPLEMENTATION 4–7 (2008).

[45] PDD-63, *supra* note 43, at *8–9.

[46] *Id.* at *2–3.

[47] *Id.*

coordinate security efforts.[48] With the input of the private sector, the Sector Liaison Official would select a "Sector Coordinator,"[49] and the two would collaborate on security initiatives. PDD-63 did not require any action from the private sector; compliance was to be voluntary.

On December 17, 2003, the Bush administration released Homeland Security Presidential Directive 7 ("HSPD-7"), which updated PDD-63 and incorporated changes from the recently passed Homeland Security Act of 2002.[50] The two documents had similar policy goals,[51] but while PDD-63 had sought to raise the status of cybersecurity efforts, HSPD-7 emphasized other physical assets and systems in addition to cybersecurity.[52]

HSPD-7 continued to rely upon the voluntary public-private partnership established by PDD-63.[53] It reiterated that the Secretary of DHS is responsible for "coordinating the overall national effort to enhance the protection of the critical infrastructure . . . ."[54] It also preserved the role of Sector-Specific (formerly "Lead") Agencies, working with the relevant associated private sectors.[55] However, HSPD-7 identified seventeen sectors, revising the twelve sector list in PDD-63.[56] Although DHS would serve as the sector-specific agency for certain sectors,[57] other sectors—such as the banking and finance sector—would have their security efforts coordinated with a more familiar department or agency.[58]

---

[48] Effective partnerships between public and private sector actors are essential, as the private sector owns approximately eighty-five percent of U.S. critical infrastructure, including financial institutions, telecommunications networks, and energy facilities. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-07-39, CRITICAL INFRASTRUCTURE PROTECTION: PROGRESS COORDINATING GOVERNMENT AND PRIVATE SECTOR EFFORTS VARIES BY SECTORS' CHARACTERISTICS 1 (2006).

[49] PDD-63, *supra* note 43.

[50] *Compare* Homeland Security Presidential Directive/HSPD-7: Critical Infrastructure Identification, Prioritization, and Protection, 2 PUB. PAPERS 1739 (Dec. 17, 2003) [hereinafter HSPD–7], *with* PDD–63, *supra* note 43, *and* Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135 (codified as amended in scattered sections of 6 U.S.C.). Notably, the Homeland Security Act did not include a definition for "critical infrastructure," and thus appeared to rely upon the relevant provision of the PATRIOT Act.

[51] *See* MOTEFF, *supra* note 44, at 16–17.

[52] *See* HSPD–7, *supra* note 50, at 1739.

[53] *See id*. at 1743 (establishing a public-private partnership in §25 of HPSD-7); *see also* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-09-654R, THE DEPARTMENT OF HOMELAND SECURITY'S (DHS) CRITICAL INFRASTRUCTURE PROTECTION COST-BENEFIT REPORT 1–2 (2009).

[54] HSPD-7, *supra* note 50, at 1740.

[55] *See id*. at 1741–42.

[56] *Id*. The directive gave the Secretary the ability to identify gaps and establish new sectors to fill these gaps. Thus, there are currently eighteen sectors: agriculture and food; defense industrial base; energy; healthcare and public health; national monuments and icons; banking and finance; water; chemical; commercial facilities; critical manufacturing; dams; emergency services; nuclear reactors, materials, and waste; information technology; communications; postal and shipping; transportation systems; and government facilities. *See generally* DHS, Critical Infrastructure and Key Resources, http://www.dhs.gov/files/programs/gc_1189168948944.shtm (last visited Apr. 12, 2010).

[57] DHS, More About the Office of Infrastructure Protection, http://www.dhs.gov/xabout/structure/gc_1189775491423.shtm (last visited Apr. 22, 2010).

[58] *See id*.

HSPD-7 and the HSA of 2002 required a "National Plan for Critical Infrastructure and Key Resources Protection," which was belatedly completed as the National Infrastructure Protection Plan ("NIPP") in 2006[59] and updated in 2009.[60] According to the NIPP, the federal government—coordinated by DHS—is supposed to work with state and local governments, as well as the owners and operators of critical infrastructure in the public and private sectors, to identify the systems and assets that comprise the country's critical infrastructure.[61] Together, these entities are to "assess those assets' vulnerabilities to the threats facing the nation . . ., determine the level of risk associated with possible attacks or the impacts of natural events on those assets, and identify and prioritize a set of measures that can be taken to reduce those risks."[62]

The NIPP identifies and integrates specific processes by which an integrated risk management effort for critical infrastructure can be developed.[63] It defines and seeks to standardize across all sectors the process for identifying and selecting assets for further analysis, identifying threats and conducting threat assessments, assessing vulnerabilities to those threats, analyzing consequences, determining risks, identifying potential risk mitigation activities, and prioritizing those activities based on cost-effectiveness.[64] The NIPP, however, does not make clear who is responsible for doing these various tasks, how and whether different types of analysis will be audited, and where ultimate authority lies. Thus, the NIPP introduces important concepts but contains little guidance for implementation.

In the *National Strategy for Homeland Security*, released in 2002, the Bush administration made clear that "[p]rimary responsibility for protection, response, and recovery lies with the owners and operators" of the particular assets and systems.[65] Unfortunately, there is nothing in this strategy or in other Executive Branch guidance that calls for verification that the proper security procedures are actually put in place.

The Homeland Security Act of 2002 also included several elements related to critical infrastructure protection.[66] The Act created the Directorate of

---

[59] DHS, NATIONAL INFRASTRUCTURE PROTECTION PLAN (2006), *available at* http://www.fas.org/irp/agency/dhs/nipp.pdf.

[60] HSPD–7, *supra* note 50, at 1743; DHS, NATIONAL INFRASTRUCTURE PROTECTION PLAN (2009), *available at* http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf [hereinafter NIPP].

[61] *See* NIPP, *supra* note 60, at 16.

[62] MOTEFF, *supra* note 44, at 2.

[63] *Id.* at 23.

[64] *See generally* NIPP, *supra* note 60.

[65] *See* NATIONAL STRATEGY FOR HOMELAND SECURITY, *supra* note 18, at 64 ("The government should only address those activities that the market does not adequately provide—for example, national defense or border security . . . . For other aspects of homeland security, sufficient incentives exist in the private market to supply protection."). It does not appear that to date the Obama administration has released a strategy trumping the Bush administration's.

[66] Homeland Security Act of 2002, Pub. L. No. 107-296, tit. II, subtit. A, §§ 201–02, 211–14, 116 Stat. 2135, 2145–55 (codified as amended at 6 U.S.C. §§ 101, 121–22, 131–33 (2006, Supp. I 2007, Supp. II 2008 & Supp. III 2009)).

Information Analysis and Infrastructure Protection.[67] However, some agencies with critical infrastructure protection responsibilities, such as the Transportation Security Administration, were not so integrated.[68] The new directorate was tasked, among other things, with receiving and analyzing "law enforcement information, intelligence information, and other information" in order to "identify and assess the nature and scope of terrorist threats to the homeland," "carry out comprehensive assessments of the vulnerabilities of the key resources and critical infrastructure of the United States, including the performance of risk assessments to determine the risks posed by particular types of terrorist attacks," and "develop a comprehensive national plan for securing the key resources and critical infrastructure of the United States . . . ."[69]

The Act gave the Directorate no authority to regulate the security of the critical infrastructure sectors enumerated in PDD-63. Even in cases where DHS had regulatory authority over a particular sector, the relevant agencies were not necessarily enveloped into the Directorate-for example, although DHS had regulatory authority over aviation, the Transportation Security Administration was not incorporated into the Directorate.[70] Therefore, the part of DHS responsible for critical infrastructure protection did not have authority over some critical infrastructure sectors within DHS. Instead, DHS had to coordinate with TSA and other agencies as if they were external to DHS.[71] Following this move, this Author heard increased concerns that the Directorate's primary responsibility was coordinative and that it lacked the authority to compel action.

The Homeland Security Act included two additional elements related to critical infrastructure protection. First, Subtitle B, "Critical Infrastructure Information," created what is now referred to as the Protected Critical Infrastructure Information ("PCII") Program.[72] This information-protection program allows private sector actors to voluntarily submit information about critical infrastructure to DHS without fear that the information will be dis-

---

[67] 6 U.S.C. § 121–22. During Secretary Michael Chertoff's "Second Stage Review," the Directorate of Information Analysis and Infrastructure Protection was reorganized. The Intelligence Analysis function became the Office of Intelligence and Analysis, and the Infrastructure Protection function became the Office of Infrastructure Protection within the National Protection and Programs Directorate. *See generally* DHS, Department Six-Point Agenda, http://www.dhs.gov/xabout/history/editorial_0646.shtm (last visited Apr. 13, 2010) [hereinafter DHS, Six-Point Agenda].

[68] MOTEFF, *supra* note 44, at 14.

[69] 6 U.S.C. § 121. This would subsequently become the National Infrastructure Protection Plan. *See* MOTEFF, *supra* note 44, at 15.

[70] *See* MOTEFF, *supra* note 44, at 14.

[71] DHS, More About the Office of Infrastructure Protection, *supra* note 57 (listing TSA as an "other agency even though it is part of the Department of Homeland Security").

[72] Homeland Security Act of 2002, Pub. L. No. 107-296, tit. II, subtit. A, §§ 211–14 116 Stat. 2135, 2150–55 (codified as amended at 6 U.S.C. §§ 101, 131–33 (2006 & Supp. I 2007)); DHS, Protected Critical Infrastructure Information (PCII) Program, http://www.dhs.gov/files/programs/editorial_0404.shtm (last visited Apr. 13, 2010) [hereinafter DHS, PCII].

closed under a disclosure law or discovered in civil litigation.[73] Information that is voluntarily submitted and not already in the public domain is exempt from disclosure, including disclosure under the Freedom of Information Act.[74] This program is meant to help DHS and its federal, state, and local partners identify critical infrastructure vulnerabilities, develop risk assessments, and enhance recovery preparedness measures.[75]

The second noteworthy provision of the Homeland Security Act is the so-called "CIPAC"[76] provision.[77] This provision, as DHS has interpreted it, enables DHS to meet with various critical infrastructure owners and operators—from both the public and private sectors—without having to report the meeting under the Federal Advisory Committee Act.[78] This provision enables the public and private sectors to work together without concern that information about threats and vulnerabilities will be reported publicly.

The Homeland Security Act sought to bring a number of critical infrastructure protection capacities to DHS without stripping authority from other departments and agencies that may regulate certain critical infrastructure sectors. The approach taken by Congress did not include regulation, but rather relied strictly upon voluntary partnerships. Unfortunately, the Act did not instruct DHS to verify that private parties were actually limiting the risk of critical infrastructure attack.[79] Moreover, mechanisms that the Act laid out to make a voluntary partnership work, like the PCII program and the CIPAC authority, have, in this Author's opinion, not been leveraged to the fullest extent.

---

[73] DHS, PCII, *supra* note 72.

[74] 6 U.S.C. § 133; *see also* Freedom of Information Act, 5 U.S.C. § 552 (2006, Supp. I 2007 & Supp. III 2009).

[75] 6 U.S.C. § 131.

[76] "CIPAC" stands for the Critical Infrastructure Partnership Advisory Council. This council was established "to facilitate effective coordination between federal infrastructure protection programs with the infrastructure protection activities of the private sector and of state, local, territorial and tribal governments." DHS, Critical Infrastructure Partnership Advisory Council, http://www.dhs.gov/files/committees/editorial_0843.shtm (last visited Apr. 13, 2010).

[77] *See* 6 U.S.C. § 121 (establishing the Directorate for Information Analysis and Infrastructure Protection); *see also id.* § 451(a) (2006) (granting DHS the ability to establish, appoint members of, and use the services of advisory committees at the Secretary's discretion).

[78] § 451(a) (stating that "[a]n advisory committee established under this section may be exempted by the Secretary from Public Law 92-463, but the Secretary shall publish notice in the Federal Register announcing the establishment of such a committee and identifying its purpose and membership"). *But see generally* Federal Advisory Committee Act, 5 U.S.C. app. §§ 9–11 (2006) (establishing rules and procedures for federal advisory committees).

[79] Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135, 2220 (instructing the Department to attempt to coordinate its activities with public and private entities but not instructing DHS to verify that private parties actually limited the risk of critical infrastructure attack).

C. Identified Problems with the Nation's Critical Infrastructure Protection Policy

DHS has not effectively leveraged the tools at its disposal to secure our critical infrastructure. The problems that have prevented it from doing so fall into three general categories: verification, bureaucracy, and value propositions.

1. Verification

DHS and its federal partners must be able to verify that the private sector is taking steps to secure critical infrastructure absent regulation. Unfortunately, CHS has had a difficult time determining whether DHS can actually verify whether enough is being done. In 2007, for example, CHS requested that DHS brief CHS on each sector and discuss the security efforts of each. In this Author's opinion, DHS struggled to definitively describe the security measures in place within a given sector. Instead, DHS stated that describing security measures was not among its responsibilities and echoed the aforementioned homeland security strategy that asserted that it was the responsibility of each asset owner to maintain security.[80] In fact, on November 13, 2009, the Secretary informed CHS that "the majority of [critical infrastructure] sites . . . cannot be compelled to provide information on protective measures."[81]

Different interpretations of the Homeland Security Act have led to different understandings of DHS's responsibility in this area. As amended, the Homeland Security Act includes the requirement that the Secretary provide Congress with an annual report discussing the security of each sector.[82] Unfortunately, the release of these reports has not always gone smoothly. For example, Congress did not receive a briefing on the 2008 report until September 2009.[83]

Moreover, the 2008 report did not adequately inform CHS of the security status of different sectors.[84] The National Annual Report should be an important document that provides Congress with a snapshot of the state of security of critical infrastructure in the United States. Compiled by public and private sector partners, the report is meant to discuss all risks to the eighteen sectors and provide a potential mechanism to better inform the prioritization of budget resources in subsequent fiscal years. Unfortunately, the

---

[80] *Cf.* NIPP, *supra* note 60, at 2.

[81] *See* Letter from Janet Napolitano, Sec'y, DHS, to CHS (Nov. 13, 2009) (on file with author).

[82] Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, tit. X, § 1002(a), sec. 201(d)(25), 121 Stat. 266, 374–75 (codified at 6 U.S.C. § 121(d)(25) (Supp. I 2007)).

[83] Letter from Bennie G. Thompson, Chairman, CHS, to Janet Napolitano, Sec'y, DHS (Sept. 25, 2009) (on file with author).

[84] *Id.*

National Annual Report has not yet provided an appropriate level of detail to fully appreciate the risks to critical infrastructure. In many cases, the report includes general statements about risks that do not account for the idiosyncrasies of each sector. Instead, these reports contain high-level language, not specifics, so it is not clear to CHS what is secured and what is not.[85] Thus, DHS's interpretation of the statutory requirements allows it to avoid giving Congress a full assessment of critical infrastructure security.

The same problems have plagued the "Sector Specific Plans" ("SSPs"), which the NIPP dictated were to be created through collaboration between government and industry.[86] In 2007, the U.S. Government Accountability Office ("GAO") reviewed nine of the plans and found that some were far more comprehensive than others.[87] Consequently, the GAO concluded that it could not assess how much progress each sector had actually made in identifying and protecting key assets.[88]

Since the 2007 GAO report, not much progress has been made. At a 2009 CHS hearing on the Mumbai attacks in early 2009,[89] CHS attempted to discern how the American equivalents of the assets that were attacked in Mumbai were secured in the United States. Testimony from DHS and hotel owners showed serious gaps not only in security, but also in verification of security measures. For example, while DHS said that New York City hotels were showing progress in security, its representative could not rank the readiness of hotels in other cities throughout the country.[90] This fact suggests that DHS is not aware of which assets are secured and that the agency does not have the information or the metrics to make such assessments.

The NIPP created a high-level plan that, at best, brought together various government and private sector groups to work on security issues. However, because it does not clearly require verification of security measures, and because DHS has not adequately conducted verification procedures, the need to verify that critical infrastructure owners and operators are securing their assets and systems has not been fulfilled.

2. Bureaucracy

Another major hurdle in implementing a coherent critical infrastructure protection strategy is the requirement of having to navigate an immense bu-

---

[85] *See id*.

[86] NIPP, *supra* note 60, at 8.

[87] *See* MOTEFF, *supra* note 44, at 24; *see also* GAO, GAO-07-706R, CRITICAL INFRASTRUCTURE PROTECTION: SECTOR PLANS AND SECTOR COUNCILS CONTINUE TO EVOLVE 3–6 (2007) [hereinafter GAO SECTOR PLANS].

[88] MOTEFF, *supra* note 44, at 24; *see also* GAO SECTOR PLANS, *supra* note 87, at 3–6.

[89] *See generally The Mumbai Attacks: A Wake-Up Call for America's Private Sector: Hearing Before the Subcomm. on Transp. Sec. and Infrastructure Prot. of the H. Comm. on Homeland Sec.*, 111th Cong. (2009) [hereinafter *Mumbai Hearing*].

[90] *See id.* at 28 (statement of James L. Snyder, Deputy Assistant Secretary, Infrastructure Protection, DHS).

reaucracy created by the need to coordinate between so many different federal departments and agencies. HSPD-7 requires that the Secretary of DHS coordinate critical infrastructure protection efforts among all of the sector-specific agencies.[91] In order to meet the requirements of the NIPP and the 9/11 Act by creating a "prioritized critical infrastructure list,"[92]—a list that dictates grant receipts[93]—departments and agencies must work together to nominate assets and systems. Although DHS is reluctant to lay blame publicly, this Author, through CHS, has discovered that departments and agencies outside of DHS frequently miss deadlines and fail to comply with the spirit of objectives in documents such as the NIPP, thus making DHS's work more difficult.

Absent intervention by the White House, DHS does not have the authority to compel these other agencies to act.[94] Especially given its relative age, it is easy to understand why DHS may be politically reluctant to publically criticize another department or agency. Moreover, if CHS were to write legislation mandating compliance from sector-specific agencies, other committees with jurisdiction over those agencies could intervene to obstruct the process.[95]

3. Value Propositions

Thus far, DHS has failed to create an effective value proposition that would show public and private sector actors why it is in their interest to invest in critical infrastructure protection. One of the greatest potential obstacles to convincing public and private sector actors to implement security measures is an incomplete understanding of the level of risk at any given facility. Risk is defined as the product of consequences of an attack, vulnerability to attack, and threat of an attack.[96] It is well-known that an attack on critical infrastructure could have grave consequences affecting lives (e.g., if a stadium or a dam were attacked), commerce (e.g., if the Mall of America or Wall Street were attacked), or morale (e.g., if the Statue of Liberty were attacked). It is also well known that some critical infrastructure, such as malls, train stations, or bridges, is vulnerable to attack. However, many places of critical infrastructure may not always have information about the third factor: the level of threat.

---

[91] *See* HSPD-7, *supra* note 50.

[92] 6 U.S.C. §§ 124l(a)(2), 609(a)(3) (Supp. I 2007 & Supp. II 2008).

[93] *See* Fiscal Year 2010 Buffer Zone Protection Program, Frequently Asked Questions, http://www.fema.gov/txt/government/grant/2010/fy10_bzpp_faq.txt (last visited Feb. 22, 2010).

[94] *See* HSPD-7, *supra* note 50 (stating that while the Secretary of DHS has the power to "coordinate," only the White House can enforce HSPD-7).

[95] *See* HOUSE RULES, *supra* note 25, at 6–16 R. X (determining the subject matter jurisdiction of house committees).

[96] *See* TODD MASSE ET AL., CONG. RESEARCH SERV., THE DEPARTMENT OF HOMELAND SECURITY'S RISK ASSESSMENT METHODOLOGY: EVOLUTION, ISSUES, AND OPTIONS FOR CONGRESS 6–7 (2007) (describing DHS's current definition of risk).

Malls present an excellent example.[97] Malls are vulnerable because entering customers are not generally screened, and the consequences of a mall attack on lives and commerce would be enormous. However, it seems that the threat—the likelihood of attack—is not sufficiently apparent to businesses for them to invest in rigorous security measures. In fact, Congress itself is often not sufficiently cognizant of risk levels: members, however concerned they may be with security, are persuaded not to require security for particular critical infrastructure lest it cost too much for the government and the private sector.[98]

CHS focused heavily on looking for effective value propositions during the 110th Congress, but the results were not as effective as they could have been. As the NIPP explained, "[i]n assessing the value proposition for the private sector, there is a clear national interest in ensuring the collective protection and resiliency of the Nation's [critical infrastructure]."[99] Unfortunately, the list of reasons provided by the NIPP for *why* companies should participate in critical infrastructure security is vague and bureaucratic. They include: "[p]articipation in both a policy development and risk analysis and management framework"[100] and "access and input into cross-sector interdependency analysis."[101] This is not the language of business, and it does not inspire participation. Until a clearer and more persuasive case can be made to business that it is in its interest to both voluntarily submit security information and to secure its critical infrastructure, business cooperation in this vital area will be limited.

---

[97] *See, e.g.*, *Ankara Blast was Suicide Bombing—Turkish Official*, BBC MONITORING EUR., May 23, 2007; Humfrey Hunter & Justin Davenport, *Suicide Bomb Woman Hits Israeli Shopping Mall as U.K. Put on Alert*, EVENING STANDARD (London), May 19, 2003, at 2. While to date no shopping malls have been successfully attacked in the United States, multiple individuals have been arrested and convicted for planning to attack American shopping malls. *See, e.g.*, Dan Eggen, *Illinois Man Charged With Plot to Wage "Jihad" in Mall*, WASH. POST, Dec. 9, 2006, http://www.washingtonpost.com/wp-dyn/content/article/2006/12/08/AR2006120800851.html; Lara Rakes Jordan, *Suspect Pleads Guilty in Ohio Mall Plot*, USA TODAY, July 31, 2007, http://www.usatoday.com/news/nation/2007-07-31-shopping-mall-plot_N.htm; Ross Kerber, *Man Charged in Plot to Attack U.S. Shopping Mall*, REUTERS, Oct. 21, 2009, http://www.reuters.com/article/idUSN21490853.

[98] *See, e.g.*, 155 CONG. REC. H12,367, 12,411 (daily ed. Nov. 5, 2009) (statement of Rep. Charlie Dent (R-Pa.)) (opposing the Chemical Facility Anti-Terrorism Act of 2009 due to the fact that "it [would] be very costly to implement" and would "affect jobs in this country"); *see also id.* at 12,412–13 (statement of Rep. Frank Lucas (R-Okla.)) (expressing concern that the Chemical Facility Anti-Terrorism Act of 2009 would have a "deep and negative impact on the agriculture industry").

[99] NIPP, *supra* note 60, at 10.

[100] *Id.*

[101] *Id.*

D. Legislative and Policy Proposals

Despite the difficulty of the problems outlined above, the policy proposals offered below attempt to provide solutions in the areas of verification, bureaucracy, and value-propositions.

1. Verification

There are several steps that the Executive Branch can and should take to verify that more is voluntarily being done to secure critical infrastructure. Because overly burdensome regulation that impedes commerce is not in the nation's best interest, especially during tough economic times, the Secretary should use legislative tools already at her disposal to verify that assets are being secured on a voluntary basis.

First, DHS should make the National Annual Reports more meaningful and analytical by providing a more detailed risk analysis of assets on the "prioritized critical infrastructure list" that is required in Title X of the 9/11 Act.[102] Though the National Annual Report is already legislatively required, the Department's interpretation of the statutory requirements should be harmonized with CHS's expectations. The report must provide detailed and comprehensive descriptions of security at critical infrastructure. Ultimately, additional legislation may be necessary to make CHS's expectations clearer.

In addition, it is also important that DHS provides clear standards for owners of critical infrastructure to follow. Title IX of the 9/11 Act includes provisions for DHS to establish a program, called the Voluntary Private Sector Preparedness Accreditation and Certification Program ("PS-Prep"), by which the Department could establish preparedness standards and private sector entities could voluntarily certify themselves against them.[103] As a FEMA fact sheet explains:

> The purpose of the PS-Prep Program is to enhance nationwide resilience in an all-hazards environment by encouraging private sector preparedness. The program will provide a mechanism by which a private sector entity—a company, facility, not-for-profit corporation, hospital, stadium, university, etcetera—may be certified by an accredited third party establishing that the private sector entity conforms to one or more preparedness standards adopted by DHS.[104]

The intent of Title IX was to follow a recommendation by the 9/11 Commission Report that a voluntary private sector preparedness program be

---

[102] 6 U.S.C. § 124l(a)(2) (Supp. I 2007).
[103] *Id.* § 321m.
[104] FEMA, Voluntary Private Sector Preparedness Accreditation And Certification Program, http://www.fema.gov/media/fact_sheets/vpsp.shtm (last visited Apr. 13, 2010).

established.[105] This voluntary mechanism could encourage critical infrastructure owners to demonstrate their implementation of security measures, thereby providing DHS more detailed information for the National Annual Report.

This Author has encountered a great deal of skepticism from private industry over this voluntary preparedness program, thus illustrating that a true partnership between the private and public sectors is not yet a reality. During the hearing on the Mumbai attacks, witnesses testified that this program could be used to ensure that critical infrastructure owners take security seriously in those sectors that are not regulated for security purposes.[106] Nevertheless, representatives from private sector firms have privately expressed concerns to the Author that this is a slippery slope toward regulation, despite the word "voluntary" in the title of the program. Furthermore, they have expressed concerns to the Author that a third party may review their proprietary information and somehow use it against them.

The claim that this voluntary accreditation system is a slippery slope toward regulation seems far-fetched. While there is an understandable concern that the establishment and acceptance of standards of preparedness within a sector could lead to liability definitions, the legislation is quite clear that the program is voluntary and not required. In fact, a failure to implement the program may galvanize Congress to regulate particular sectors because those sectors will not participate in such voluntary schemes. It behooves companies to participate and help define the boundaries of the accreditation program, rather than waiting for a visceral response to tragedy from a Congress which will surely be less susceptible to negotiation. Furthermore, DHS can assuage concerns about the misuse of proprietary information by promoting and leveraging the aforementioned PCII Program.[107]

In order for both of these goals—better information on the status of critical infrastructure and implementation of a voluntary accreditation program—to be met, Congress must work together with the private sector. This could be an unusual chance for government to join with the private sector in a security program to the benefit of both. However, in order for that to happen, the government must build trust and be creative. Tools such as the PCII Program and the CIPAC exemption, which facilitate the exchange of information between the public and private sectors, could be leveraged to protect sensitive information and help establish mutual trust.

Unfortunately, some recent actions by DHS have undermined these goals. This Author believes that DHS has failed to meet several deadlines related to the PS-Prep program. The private sector will participate in these initiatives only if owners feel that critical infrastructure protection is in their

---

[105] *See* H.R. Rep. No. 110-259, at 322–23 (2007), *reprinted in* 2007 U.S.C.C.A.N. 119; *see also* 9/11 Commission Report, *supra* note 23, at 398.

[106] *See generally Mumbai Hearing*, *supra* note 89.

[107] *See supra* notes 72–75 and accompanying text.

own interest and important to the security of the country. Therefore, it is important to bring the failure of the PS-Prep program to light in order to encourage DHS and the private sector to start work on the program, even if only in a series of pilot programs.

Finally, though the voluntary framework is ideal, Congress should never take regulation of critical infrastructure sectors off of the negotiating table. If the voluntary framework fails because DHS lacks the ability to verify the security measures in place, regulation by Congress might be necessary.

Some sectors have already been regulated for security purposes. For example, following the September 11 attacks, several chemical sector experts—including experts from the chemical industry itself—supported security regulation.[108] The rationale for regulation was multi-faceted. First, chemical facilities possess materials that could cause serious harm to people. Second, some facilities were close to large metropolitan centers. Finally, common chemicals can be used for devastating terrorist attacks.[109] The regulatory regime imposed on the chemical sector, while successful in many ways, did encounter jurisdictional obstacles, as evidenced by water and wastewater facilities being exempted from the legislation.[110] H.R. 2868, passed in the 111th Congress, eliminates these exceptions.[111] It is an excellent example of multiple committees working together to pass comprehensive, risk-based homeland security legislation.

Congress can point to the paradigm of the chemical facility security experience when explaining to the private sector what security regulation might look like. This successful model shows that, if it did become necessary, regulation could be a possible solution to critical infrastructure security concerns.

2. Bureaucracy

Among the major weaknesses in our nation's critical infrastructure policy is the inability of federal bureaucracies to work together to protect critical infrastructure, even despite HSPD-7's explicit call for meaningful cooperation.[112] As discussed previously, one of the central problems with the

---

[108] *See, e.g.*, American Chemistry Council, Chemical Security Issue Brief, http://www.americanchemistry.com/s_acc/sec_article_acc.asp?CID=258&DID=10008 (last visited Apr. 13, 2010) ("ACC continues to be a strong advocate for federal security regulations to ensure that nationwide, all high-risk chemical facilities take the same steps our members have to enhance security.").

[109] PAUL ORUM, CTR. FOR AM. PROGRESS, CHEMICAL SECURITY 101: WHAT YOU DON'T HAVE CAN'T LEAK OR BE BLOWN UP BY TERRORISTS 1 (2008), *available at* http://www.americanprogress.org/issues/2008/11/pdf/chemical_security.pdf.

[110] Department of Homeland Security Appropriations Act, Pub. L. No. 109-295, § 550, 120 Stat. 1355, 1388–89 (2006) (codified as amended at note following 6 U.S.C. § 121 (Supp. III 2009)).

[111] *See* Chemical Facility Anti-Terrorism Act of 2009, H.R. 2868, 111th Cong. (2009).

[112] *See generally* HSPD-7, *supra* note 50.

implementation of the NIPP is that DHS cannot force its federal partners to comply.[113] As a result, DHS often does not receive sectors' annual plans and information in a timely manner.

Given this problem, DHS should be required to report to Congress each time one of its federal partners fails to comply with a deadline or objective in the NIPP. This would raise awareness and put public pressure on federal partners to meet the goals called for in the Homeland Security Act, HSPD-7, and the NIPP. Although DHS should support such legislation, the legislation may encounter opposition from DHS's federal partners and also from the private sector, which may be wary of any potential for additional oversight. In fact, Congress itself may create some barriers to the adoption of this proposal, as enacting such legislation would require the assent of several congressional committees with jurisdiction over a federal department or agency identified in the NIPP, each of which would want to write the rules in a manner that protects the interests of the department or agency that it primarily oversees. This is an area where consolidation of jurisdiction over DHS in a single committee would help avoid bureaucratic red tape and more efficiently solve the problem. Despite these hurdles, a process can and should be legislatively crafted to require DHS to report when its partners fail to comply with the NIPP.

3. Value Proposition

Unless the risk to our critical infrastructure clearly and dramatically increases or regulation becomes politically feasible, we will likely rely upon a voluntary framework to secure most of our critical infrastructure for the foreseeable future. In addition to the aforementioned means to bolster voluntary cooperation—for example, the PS-Prep program—DHS must create a meaningful value proposition that will encourage private sector owners and operators to make significant investments in security and to tell DHS about their progress.

The Committee has devoted extensive resources to constructing an effective value proposition for investments in the security of critical infrastructure, even though a profit may not result.[114] In the absence of relevant threat information, critical infrastructure owners and operators will likely not invest in security unless they receive some form of government support or unless it can be shown that such investment would improve their businesses (for example, by giving businesses a metric to assess the preparedness of their suppliers). An ideal value proposition should explain how investments in security help the efficacy of supply chains, boost employee morale, and

---

[113] *See* discussion *supra* Part III.C.2.

[114] *See generally, e.g.*, *Partnering Hearing*, *supra* note 21; *Resilient Hearing*, *supra* note 21.

ensure that companies that suffer a disruption can successfully remain in business.[115]

Recognizing these difficulties, CHS began to focus on a strategy based upon "resilience," which concerns the ability of a disrupted asset or system to return to business quickly. A 2007 report by the Council on Economic Competitiveness, entitled *The Resilient Economy: Integrating Competitiveness and Security*, found that the 835 companies that announced a supply chain disruption between 1989 and 2000 experienced thirty-three to forty percent lower stock returns than did their industry peers.[116] These findings clearly indicate that to keep one's business at acceptable profit levels, disruptions must be avoided or minimized.

By investing in measures to mitigate disruptions, firms would also be getting at the root of the risk caused by a security event. After the September 11 attacks, the private sector suffered most of the record eighty billion dollars in economic losses.[117] If those firms were more resilient—whether in their supply-chains or employee telecommuting policies—they may have suffered smaller economic losses.

The Committee therefore suggested a resilience strategy for critical infrastructure protection that would promote protection and the quick ability to reconstitute and continue operations; however, the Bush administration declined to adopt it.[118] Through the concept of resilience, however, there may be a way of helping the bottom-line of companies while providing a security benefit. In short, DHS would engage the private sector to promote security measures by asserting that the minimization of the effects of disruptions would not only help to promote national security but would also help their bottom-lines. Rather than a particular program, this could take the form of a strategy implemented as part of many DHS programs.

These proposals demonstrate that a more effective approach to critical infrastructure security does not require a broad-scale change, but merely the creative leveraging of existing mechanisms in a manner that compels private-sector partners to act. In some cases, the solution is as simple as aligning DHS's interpretation of statutes with the intent of Congress. If these interpretations do not change under the Obama administration, additional legislation may be needed to help DHS more effectively navigate the byzan-

---

[115] *See Hewlett-Packard Features Enterprise Resilience: Turning Security Costs Into Business Advantages*, COMPETE.ORG, Nov. 29, 2007, http://www.compete.org/news/entry/351/hewlett-packard-features-enterprise-resilience/; *see also* DEBRA VAN OPSTAL, COUNCIL ON COMPETITIVENESS, TRANSFORM—THE RESILIENT ECONOMY: INTEGRATING COMPETITIVENESS AND SECURITY (2007), *available at* http://www.compete.org/images/uploads/File/PDF%20Files/Transform_The_Resilient_Economy_FINAL_pdf.pdf.

[116] OPSTAL, *supra* note 115, at 6.

[117] *See Partnering Hearing, supra* note 21, at 1 (statement of Sheila Jackson Lee, Member, CHS).

[118] *See Resilient Hearing*, *supra* note 21, at 1 (statement of Rep. Thompson, Chairman, H. Comm. on Homeland Sec.) ("The business community must have cutting-edge technology in order to effectively bounce back.").

tine scheme of Congress's homeland security legislation, perhaps by consolidating control in one committee. America's adversaries have demonstrated a serious and creative commitment to attacking U.S. infrastructure. Congress, the Executive Branch, and the private sector must all be equally creative in securing these assets and systems.

IV. Disaster Preparedness and Response

The forces of both Mother Nature and man will always pose a danger to our civilization. Ideally, the warnings of an impending disaster would come days in advance. More often, however, disasters provide little notice, as in the case of an earthquake, tornado, tsunami, or terrorist attack.[119] Regardless of the type of disaster, the end result is usually the same: destruction, misery, and death.[120]

Another constant in disasters is the courageous action of first responders and preventers: firefighters, police, emergency medical technicians, and a host of volunteer groups and nongovernmental organizations.[121] Their activities may seem routine—rescuing the injured, extinguishing fires, securing the area, and restoring order[122]—but the chaos that surrounds a disaster is no ordinary matter. Officials from local and state governments have primary responsibility for disaster response and usually arrive immediately after an event.[123] However, if they become overwhelmed and unable to respond adequately to a disaster, the governor of a state may request assistance from the federal government.[124]

This Part first discusses the evolution of federal emergency response in America and then presents several legislative proposals: consolidated jurisdiction, a stronger FEMA within DHS, terrorism preparedness, an empowered citizenry, and disaster mitigation.

A. Background

A successful emergency management system must respond to the needs of all people in a timely and accountable manner and must engage communities and stakeholders alike, so that the citizenry becomes an integral part of

---

[119] *See, e.g.*, George Haddow & Jane Bullock, Introduction to Emergency Management 30 (3d ed. 2008) (describing earthquakes as "sudden events" in spite of scientists' best efforts to predict their occurrence).

[120] Ad Hoc Subcomm. on Disaster Recovery of the S. Comm. on Homeland Sec. & Governmental Affairs, 111th Cong., Far From Home: Deficiencies in Federal Disaster Housing after Hurricanes Katrina and Rita and Recommendations for Improvement 25 (Comm. Print 2009) [hereinafter Far From Home].

[121] *See* Haddow & Bullock, *supra* note 119, at 99.

[122] *Id.*

[123] *See* GAO, GAO-09-811, Disaster Recovery: Experiences from Past Disasters Offer Insights for Effective Collaboration After Catastrophic Events 3 (2009).

[124] Haddow & Bullock, *supra* note 119, at 113–14.

securing the homeland from threats of all types of hazards. The following paragraphs briefly describe issues common to all disasters and the method for emergency assistance, outline the rapid evolution of emergency response in America, and conclude with several legislative proposals this Author has supported in Congress.

1. Legislating the Federal Response

Historically, Congress provided federal assistance to states, localities, and victims in an ad hoc manner after a disaster, authorizing funds or directing federal personnel and equipment to respond to each event.[125] Federal assistance proved popular, but the piecemeal approach to disaster assistance was inefficient and difficult to manage.[126] To resolve these issues, Congress created a comprehensive scheme for federal disaster relief in the Disaster Relief Act of 1950, which gave the President considerable power to prescribe and coordinate emergency assistance to states and localities.[127] The Disaster Relief Acts of 1970[128] and 1974[129] further extended the federal assistance available for individuals, states, and local communities suffering from disasters.

While the laws directing disaster relief consolidated response efforts, the agencies that carried out emergency preparedness, mitigation, and response remained spread throughout the federal government.[130] In the 1970s, for instance, emergency management functions were performed directly by at least five federal departments and agencies, and more than one hundred federal agencies were tangentially involved in disasters and emergency response.[131] Numerous natural disasters in the 1970s, along with a highly publicized emergency at the Three Mile Island Nuclear Power Plant in Pennsylvania, exposed significant weaknesses in the federal government's emergency response framework and ultimately prompted President Carter to

---

[125] *See* FAR FROM HOME, *supra* note 120, at 25; *see also* HENRY B. HOUGE & KEITH BEA, CONG. RESEARCH SERV., FEDERAL EMERGENCY MANAGEMENT AND HOMELAND SECURITY ORGANIZATION: HISTORICAL DEVELOPMENTS AND LEGISLATIVE OPTIONS 5 (2006) [hereinafter FEDERAL EMERGENCY MANAGEMENT]; FEMA, FEMA History, http://www.fema.gov/about/history.shtm (last visited Apr. 13, 2010) [hereinafter FEMA History].

[126] FEMA History, *supra* note 125.

[127] Disaster Relief Act of 1950, Pub. L. No. 81-875, 64 Stat. 1109 (repealed 1970).

[128] Disaster Relief Act of 1970, Pub. L. No. 91-606, 84 Stat. 1744 (codified as amended in scattered sections of 42 U.S.C.).

[129] Disaster Relief Act of 1974, Pub. L. No. 93-288, 88 Stat. 143 (codified as amended at 42 U.S.C. §§ 5121–207 (2006, Supp. I 2007 & Supp. II 2008)).

[130] For an exhaustive history of emergency management in the United States, *see* FEDERAL EMERGENCY MANAGEMENT, *supra* note 125, at 4–25.

[131] The federal agencies involved in disaster and emergency response included the Department of Commerce, the General Services Administration, the Treasury Department, the Nuclear Regulatory Commission, and the Department of Housing and Urban Development. HADDOW & BULLOCK, *supra* note 119, at 5.

call for a reorganization of the federal government's emergency response efforts.[132]

In 1978, President Carter submitted Reorganization Plan Number 3 ("Plan Number 3") to Congress, which established the Federal Emergency Management Agency ("FEMA").[133] Congress subsequently adopted the plan,[134] and Executive Order 12,127 officially established FEMA on March 31, 1979.[135] For the first time, key emergency management and assistance functions would be unified at the federal level and made directly accountable to the President and Congress.

FEMA is responsible for coordinating the federal government's disaster relief efforts, including planning, protection, preparedness, response, recovery, and mitigation.[136] FEMA's authority to respond to disasters was consolidated by the Robert T. Stafford Disaster Relief and Emergency Assistance Act, the nation's primary law for disaster assistance.[137] Under the Act, the President is authorized to declare an incident either a "major disaster"[138] or "emergency,"[139] which dictates the type and level of federal aid available to states, localities, and individual victims. Before the President makes a declaration, however, the governor of the affected state must request assistance by stating that the incident is of such severity and magnitude that effective response is beyond state or local capabilities.[140] The President also has discretion to provide federal assistance without a gubernatorial request if the emergency involves a subject area or responsibility exclusively within the

---

[132] *See* FAR FROM HOME, *supra* note 120, at 28; HADDOW, *supra* note 119, at 5.

[133] Reorganization Plan No. 3 of 1978, 3 C.F.R. 329 (1979), *reprinted in* note following 15 U.S.C. § 2201 (2006), *and in* 92 Stat. 3788 (1978).

[134] The previous year, in 1977, Congress passed the Reorganization Act of 1977, which stated that a reorganization plan would be effective if Congress either defeated or did not pass a measure of disapproval within sixty days of receiving the President's Reorganization plan. *See generally* Reorganization Plan of 1977, Pub. L. No. 95-17, 91 Stat. 29 (codified as amended at 5 U.S.C. §§ 901–12 (2006)). Following the presentment of President Carter's Reorganization Plan of 1978, the House defeated a measure of disapproval and the Senate never voted on it. As a result, President Carter's plan took effect. *See* H. Res. 1242, 95th Cong. (1978) (disapproving of Reorganization Plan No. 3, which failed House by vote of 327-40); S. Res. 489, 95th Cong. (1978) (disapproving of Reorganization Plan No. 3, which failed the House by a vote of 327-40).

[135] Exec. Order 12,127, 3 C.F.R. 376. Executive Order 12,148, 3 C.F.R. 412 (1980), required reassignment of agencies, program, and personnel to the new entity.

[136] According to FEMA's website, FEMA's mission is to support our citizens and first responders to ensure that as a nation we work together to build, sustain, and improve our capability to prepare for, protect against, respond to, recover from, and mitigate all hazards. *See* FEMA, About FEMA, http://www.fema.gov/about/index.shtm (last visited Apr. 13, 2010).

[137] 42 U.S.C. §§ 5121–208 (2006, Supp. I 2007 & Supp. II 2008).

[138] *Id.* § 5170.

[139] *Id.* § 5191. The President may issue an emergency declaration without a gubernatorial request if primary responsibility for response rests with the federal government generally because the subject matter at issue is the preeminent responsibility of the United States. § 5191(b).

[140] §§ 5170, 5191.

federal domain.[141] Under certain circumstances, the President is authorized to pre-position equipment and personnel and direct the performance of emergency work before an incident occurs.[142]

Once the President makes a declaration, authority for disaster relief operations descends from the President to FEMA.[143] The Act grants broad "general federal assistance" authority to the President, empowering him to "direct any Federal agency, with or without reimbursement, to utilize its authorities and the resources granted to it under Federal law . . . in support of State and local assistance response and recovery efforts,"[144] and to "coordinate all disaster relief assistance provided by Federal agencies, private organizations, and State and local governments . . . ."[145] The Act further authorizes "essential assistance" during major disaster declarations in order to prevent immediate threats to life and property in the form of emergency shelter, search and rescue, lending or donating of federal equipment, distribution (through state and local governments and voluntary organizations) of medicine and food, and clearing debris, among other things.[146] Other forms of permitted assistance include hazard mitigation grants to reduce future risks and damages,[147] federal facilities repair and reconstruction,[148] and repair, restoration, and replacement of damaged facilities owned by state and local governments and owners of private nonprofit facilities that provide essential services.[149] Section 408 of the Act authorizes housing and financial assistance for individuals, including medical, dental, and personal property expenses.[150]

---

[141] § 5191(b). The President used this special authority to provide assistance for the fires and explosions on September 11, 2001, and the loss of the Space Shuttle Columbia on February 1, 2003. *See* Notice, 66 Fed. Reg. 48,682 (Sept. 21, 2001) (9/11 Attacks in Virginia); Notice, 68 Fed. Reg. 9667 (Feb. 28, 2003) (Space Shuttle Columbia).

[142] *See, e.g.*, 42 U.S.C. §§ 5170b(c), 5187; *see also* KEITH BEA, CONG. RESEARCH SERV., FEDERAL STAFFORD ACT DISASTER ASSISTANCE: PRESIDENTIAL DECLARATIONS, ELIGIBLE ACTIVITIES, AND FUNDING (2010).

[143] *See* Exec. Order No. 12,148, 3 C.F.R. 412 (1980). The Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135 (codified as amended in scattered sections of 6 U.S.C.), moved FEMA into the newly created DHS. Section 52 of Executive Order 13,286 amends Executive Order 12,148 to reflect this change. 3 C.F.R. 166, 177 (2004); *see also* FAR FROM HOME, *supra* note 120, at 35.

[144] 42 U.S.C. § 5170a(1) (2006).

[145] § 5170a(2).

[146] *Id.* § 5170b. Similar "essential assistance" is permitted for "emergency declarations" made by the President. *See id.* § 5192.

[147] *Id.* § 5170c; *see also* 42 U.S.C. § 5133 (2006 & Supp. II 2008) (describing pre-disaster mitigation).

[148] 42 U.S.C. § 5171 (2006).

[149] *Id.* § 5172.

[150] Disaster Relief Act of 1974, Pub. L. No. 93-288, § 408, 88 Stat. 143, 156 (codified as amended at 42 U.S.C. § 5174 (2006)).

2. Today's FEMA

Like many federal agencies, FEMA and emergency management generally has evolved to respond to the most prevalent threats at any given time in history. Throughout the Cold War, for example, civil defense was a priority and emergency management centered on the threat of nuclear weapons.[151] In the late 1970s and early 1980s, FEMA's first director, John Macy, attempted to implement an all-hazards approach by underscoring similarities between natural hazards, preparedness, and civil defense, but a national security focus soon eclipsed FEMA's other priorities again after President Ronald Reagan took office.[152] President Clinton's FEMA Director, James Lee Witt, reemphasized an all-hazards, comprehensive emergency management approach and refocused the agency's mission on quick responses to natural disasters, despite many calls to address terrorism issues more formally.[153]

September 11 changed emergency management in the United States forever.[154] Terrorism initially gained the attention of emergency planners during the 1972 Munich Olympics[155] and resurfaced periodically during the Reagan, George H.W. Bush, and Clinton presidencies,[156] but it did not become a major focus until September 11 ushered in a massive overhaul of federal priorities and organization.[157] Title V of the Homeland Security Act created the Emergency Preparedness and Response ("EPR") Directorate at DHS[158] and transferred the functions and personnel of six existing entities, the largest of which was FEMA, to DHS.[159] Section 507 of the Act specifi-

---

[151] Patrick S. Roberts, *FEMA and the Prospects for Reputation-Based Autonomy*, 20 STUD. AM. POL. DEV. 57, 58–59 (2006). To respond, President Harry S. Truman established the Federal Civil Defense Administration ("FCDA") by executive order. Exec. Order No. 10,186, 15 Fed. Reg. 8557 (Dec. 5, 1950); *see also* FEDERAL EMERGENCY MANAGEMENT, *supra* note 125, at 6.

[152] *See* CHARLES PERROW, THE NEXT CATASTROPHE 54–55 (2007); Roberts, *supra* note 151, at 61–62.

[153] *See* Roberts, *supra* note 151, at 69–70, 73; *see also* HADDOW & BULLOCK, *supra* note 119, at 11. Preceding Administrator Witt's transformation of FEMA, Vice President Al Gore submitted a National Performance Review to President Clinton in September 1993, which reviewed numerous government programs and issues and included four recommendations related to FEMA. FEDERAL EMERGENCY MANAGEMENT, *supra* note 125, at 17 (discussing NAT'L PERFORMANCE REVIEW, OFFICE OF THE VICE PRESIDENT, FROM RED TAPE TO RESULTS: CREATING A GOVERNMENT THAT WORKS BETTER & COSTS LESS 140 (1993)). The review called for shifting FEMA's resources and focus from preparedness for nuclear war to preparation for all types of disasters. *Id.*

[154] *See* HADDOW & BULLOCK, *supra* note 119, at 303, 376; *see also* FAR FROM HOME, *supra* note 120, at 35.

[155] *See* Roberts, *supra* note 151, at 62 (noting that the terrorist attack at the 1972 Munich Olympics motivated emergency planners to re-examine and fortify their response to a terrorist attack).

[156] *See* Charles Perrow, *Using Organizations: The Case of FEMA, Homeland Security Affairs*, HOMELAND SECURITY AFF., Fall 2005, at 2–3.

[157] *See* Roberts, *supra* note 151, at 62.

[158] Homeland Security Act of 2002, Pub. L. No. 107-296, tit. V, § 501, 116 Stat. 2135, 2212 (codified as amended at 6 U.S.C. § 311 (2006 & Supp. I 2007)).

[159] *Id.* § 503, 116 Stat. at 2213 (codified as amended at 6 U.S.C. § 313 (2006)).

cally charged FEMA with "carrying out its mission to reduce the loss of life and property and protect the Nation from all hazards by leading and supporting the Nation in a comprehensive, risk-based emergency management program."[160] A subsequent reorganization by DHS Secretary Michael Chertoff eliminated EPR, made FEMA and its new director (formerly the Undersecretary for EPR) directly report to the Secretary, and separated FEMA's preparedness functions from its response and recovery functions, moving the preparedness functions into a newly created Preparedness Directorate.[161]

FEMA's intense focus on new homeland security priorities and its subsequent reorganizations within DHS seem to have overwhelmed the agency.[162] FEMA's focus shifted to encompass homeland security matters more broadly with a number of new programs and grants,[163] including the State Homeland Security Grant Program ("SHSGP") and the Urban Areas Security Initiative ("UASI"), both designed to direct millions of dollars to help communities face the threat of terrorism.[164] A report by the GAO showed that "almost three of every four grant dollars appropriated to the [Department of Homeland Security] for first responders in fiscal year 2005 were for three primary programs that had an explicit focus on terrorism."[165] In 2004, only two out of 222 FEMA training exercises involved hurricanes, demonstrating that the emphasis on terrorism had definitely bled into FEMA's training exercises as well.[166] With such a fundamental shift in priorities, many proponents of "all hazards emergency management" were concerned that the country was becoming more vulnerable to natural disasters.[167] In its first major test, the reorganized system failed.[168]

---

[160] *Id.* § 507, 116 Stat. at 2214–15 (codified as amended at 6 U.S.C. § 317 (2006 & Supp. I 2007)).

[161] *See generally* DHS, Six-Point Agenda, *supra* note 67; *see also* FEDERAL EMERGENCY MANAGEMENT, *supra* note 125, at 17–18.

[162] *See* HADDOW & BULLOCK, *supra* note 119, at 306; PERROW, *supra* note 152, at 97, 118; Roberts, *supra* note 151, at 76.

[163] *See* FAR FROM HOME, *supra* note 120, at 35; FEMA History, *supra* note 125; *see also* STAFF OF S. COMM. ON HOMELAND SEC. AND GOV'T AFFAIRS, 109TH CONG., HURRICANE KATRINA—A NATION STILL UNPREPARED 221–24 (Comm. Print 2006) [hereinafter A NATION STILL UNPREPARED].

[164] Indeed, out of the types of assistance programs offered by the Department in fiscal years 2008 and 2009, ten out of seventeen programs could be categorized as terrorism preparedness programs. In fiscal year 2010, eight out of fifteen programs were categorized as terrorism preparedness programs. *See* SHAWN REESE, CONG. RESEARCH SERV., DEPARTMENT OF HOMELAND SECURITY ASSISTANCE TO STATES AND LOCALITIES: A SUMMARY AND ISSUES FOR THE 111TH CONGRESS 14 (2009).

[165] *See* GAO, GAO-05-652, HOMELAND SECURITY: DHS' EFFORTS TO ENHANCE FIRST RESPONDERS' ALL-HAZARDS CAPABILITIES CONTINUE TO EVOLVE 36 (2005).

[166] *See* Lisa Myers, *Was FEMA Ready for a Disaster Like Katrina?*, MSNBC, Sept. 2, 2005, http://www.msnbc.msn.com/id/9178501/.

[167] *See* HADDOW & BULLOCK, *supra* note 119, at 376, 146; *see also Exposed by Katrina, FEMA's Flaws Were Years in Making*, USA TODAY, Sept. 7, 2005, http://www.usatoday.com/news/opinion/editorials/2005-09-07-our-view_x.htm.

[168] *See* A NATION STILL UNPREPARED, *supra* note 163, at 2 ("These failures were not just conspicuous; they were pervasive."); HADDOW & BULLOCK, *supra* note 119, at 22 ("by any objective evaluation of the response [to Hurricane Katrina], it was a colossal failure").

3. The Darkest Hours

In August 2005, Hurricane Katrina made landfall along the Gulf of Mexico.[169] A major Category Three storm,[170] Katrina severely battered the coasts of Mississippi, Alabama, and Louisiana and created a storm surge that breached the New Orleans levee system.[171] Hurricane Katrina was among the costliest and deadliest natural disasters in U.S. history, with approximately eighty billion dollars in damages and a death toll of approximately 1800.[172] In many ways, Hurricane Katrina was FEMA's "perfect storm," a large-scale disaster that showcased how ineffective leadership, poor communication between the Director and the White House, and a significant change in the agency's focus can thoroughly undermine a federal response. The numerous shortfalls in budget, staffing, judgment, planning, and leadership that contributed to the devastation of Mississippi and others in the region are well documented.[173] It seemed FEMA lacked the capacity to coordinate the federal response to a catastrophe the size of Katrina.[174]

Following Katrina, Congress passed the Post Katrina Emergency Reform Act of 2006 ("PKEMRA"), which was attached to the DHS Appropriations Act of 2007 and signed into law on October 4, 2006.[175] PKEMRA

---

[169] A NATION STILL UNPREPARED, *supra* note 163, at 21.

[170] Hurricanes are separated into five categories on the Saffir-Simpson Scale depending on wind speed, storm surge, and potential damage. *See* A NATION STILL UNPREPARED, *supra* note 163, at 45 n.2. Hurricane Katrina made landfall as a Category Three storm, but it had begun delivering strong winds and driving its storm surge in the Gulf of Mexico when it was a Category Five. *Id.* at 21.

[171] *See generally* Willie Drye, *Hurricane Katrina: The Essential Time Line*, NAT'L GEOGRAPHIC NEWS, Sept. 14, 2005, http://news.nationalgeographic.com/news/2005/09/0914_050914_katrina_timeline.html (describing the path of Hurricane Katrina, stating that on Monday, August 29, at 8:00 a.m., New Orleans Mayor Ray Nagin reported water from Hurricane Katrina breaching the city's levee system, and noting that three hours later, a levee failed and the city began to flood).

[172] *See* AXEL GRAUMANN ET AL., NAT'L OCEANIC & ATMOSPHERIC ADMIN., HURRICANE KATRINA: A CLIMATOLOGICAL PERSPECTIVE 3 (2005), *available at* http://www.ncdc.noaa.gov/oa/reports/tech-report-200501z.pdf (noting that the death toll of Hurricane Katrina was approximately 1833 and represented the third deadliest hurricane in the United States since 1900); HADDOW & BULLOCK, *supra* note 119, at 35; GAO, GAO-06-618, CATASTROPHIC DISASTERS: ENHANCED LEADERSHIP, CAPABILITES, AND ACCOUNTABILITY CONTROLS WILL IMPROVE THE EFFECTIVENESS OF THE NATION'S PREPAREDNESS, RESPONSE, AND RECOVERY SYSTEM 10–11 (2006) [hereinafter GAO, CATASTROPHIC DISASTERS: PREPAREDNESS] (noting eighty billion in damages).

[173] *See* HADDOW & BULLOCK, *supra* note 119, at 35; *see also* H.R. REP. NO. 109-377 (2006); GAO, CATASTROPHIC DISASTERS: PREPAREDNESS, *supra* note 172, at 10–11 (stating that the capabilities of federal, state and local authorities were overwhelmed and observing that responders "encountered significant breakdowns in vital areas such as emergency communications as well as obtaining and deploying essential supplies and equipment"); FAR FROM HOME, *supra* note 120; A NATION STILL UNPREPARED, *supra* note 163; WHITE HOUSE, THE FEDERAL RESPONSE TO HURRICANE KATRINA: LESSON LEARNED (2006).

[174] *See* A NATION STILL UNPREPARED, *supra* note 163, at 224 (discussing FEMA Director Michael Brown's discussions with DHS leadership and White House personnel that FEMA could not respond to a catastrophe).

[175] Post Katrina Emergency Reform Act of 2006, Pub. L. No. 109-295, tit. VI, 120 Stat. 1355, 1394–463 (codified in scattered sections of 6 U.S.C.).

made FEMA a distinct agency within DHS and placed restrictions on the Secretary's authority to reorganize it,[176] directed the Administrator to respond directly to the Secretary,[177] created a direct line of communication between the Administrator and the President during times of emergency,[178] and reintegrated preparedness and response and recovery operations into one entity: FEMA.[179] With these new legislative mandates, FEMA is now better positioned to fulfill its mission to protect America from all hazards, including natural disasters, acts of terrorism, and other man-made catastrophes.[180] FEMA's renewed sense of purpose should enable the agency to prosper within DHS and foster stronger partnerships with communities.

B. Proposals

Notwithstanding Congress's direct legislative response to Hurricane Katrina, congressional oversight of FEMA in the House remains bifurcated primarily between CHS and the Committee on Transportation and Infrastructure ("T&I").[181] Under Rule X of the Rules of the House of Representatives, CHS has jurisdiction over the "domestic preparedness for and collective response to terrorism,"[182] while T&I may assert jurisdiction over "[f]ederal management of emergencies and natural disasters"[183] more broadly.[184] Such a splitting of legislative oversight lends itself to inefficiency and unnecessary complexity, particularly when viewed against PKEMRA's mandate for a "risk-based, *all hazards strategy*," by FEMA.[185] Now that FEMA is an

---

[176] *Id.* § 611, 120 Stat. at 1395–410 (codified as amended at 6 U.S.C. § 311–21m (2006, Supp. I 2007 & Supp. II 2008)) (amending tit. V of the Homeland Security Act of 2002); § 611, sec. 506(a), 120 Stat. at 1400 (codified at 6 U.S.C. § 316(a)) (distinct entity within DHS); § 611, sec. 506(c), 120 Stat. at 1400 (codified at 6 U.S.C. § 316(c)) (prohibition on reorganization authority).

[177] § 611, sec. 503(c)(3), 120 Stat. at 1397 (codified at 6 U.S.C. § 313(c)(3)) (report directly to Secretary).

[178] § 611, sec. 503(c)(5), 120 Stat. at 1398 (codified at 6 U.S.C. § 313(c)(5)) (cabinet status during disasters); § 611, sec. 503(b), 120 Stat. at 1396–97 (codified at 6 U.S.C. § 313(b)) (integrating preparedness into FEMA mission).

[179] § 611, sec. 503(b) (integrating preparedness into FEMA mission). FEMA's preparedness and response functions were separated under Secretary Chertoff's early tenure at the Department during his Second-Stage Review. *See generally* DHS, Six-Point Agenda, *supra* note 67.

[180] Homeland Security Act of 2002, Pub. L. No. 107-296, tit. V, § 502, 116 Stat. 2135, 2212–13 (codified as amended at 6 U.S.C. § 314).

[181] The Committee on Financial Services has primary jurisdiction over FEMA's flood insurance responsibilities. *See* HOUSE RULES, *supra* note 25, at 7 R. X.1(g)(4) (granting the House Committee on Financial Services jurisdiction over "insurance generally").

[182] *Id.* at 7 R. X.1(i)(3)(D).

[183] *Id.* at 8 R. X.1(r)(2).

[184] Interestingly, T&I's jurisdiction under Rule X contains no exception for terrorism-related jurisdiction of CHS. *See id.* at 8–9 R. X.1(r). For example, where CHS and the House Judiciary Committee share jurisdiction over border and port security, Rule X creates an explicit exception in CHS jurisdiction for "immigration policy and non-border enforcement." *Id.* at 7 R. X.1(i)(3)(A).

[185] 6 U.S.C. § 313(b)(2)(H) (2006) (emphasis added).

essential component of DHS, jurisdiction of FEMA should be consolidated within CHS.

FEMA, at a minimum, must have the leadership and resources to serve as an emergency management facilitator at the national level, while simultaneously empowering local, state, and federal authorities to respond efficiently during crises.[186] To this end, the author introduced the Plan to Restore Excellence and Professional Accountability in Responding to Emergencies Act, H.R. 4840, in the 109th Congress, which would have: (1) required the FEMA Administrator to possess experience in emergency management; (2) organized DHS to allow the Administrator to report directly to the President during all incidents of national significance; and (3) reunited the preparedness and response functions within FEMA.[187] PKEMRA incorporated these proposals and several other improvements to our emergency management system, making FEMA a stronger agency within DHS and an integral component of the homeland security mission.[188]

Despite the clear evidence from Katrina that FEMA needs to recalibrate its all-hazards approach to better prepare for natural disasters, the possibility of another terrorist attack in the United States also cannot be ignored. Accordingly, CHS navigated the jurisdictional interests of seven other House Committees[189] to authorize the SHSGP[190] and UASI[191] grant programs in the

---

[186] *See generally PKEMRA Implementation: An Examination of FEMA's Preparedness and Response Mission: Hearing Before the Subcomm. on Emergency Commc'ns, Preparedness, and Response of the H. Comm. on Homeland Sec.*, 111th Cong. (2009).

[187] *See* H.R. 4840, 109th Cong. (2006). The National Emergency Management Reform and Enhancement Act of 2006 also incorporated many provisions originally proposed in H.R. 4840. *See* H.R. 5351, 109th Cong. (2006).

[188] Post Katrina Emergency Management Reform Act of 2006, Pub. L. No. 109-295, tit. VI, § 611, 120 Stat. 1355, 1395–410 (codified as amended at 6 U.S.C. §§ 311–21m, 701 (2006, Supp. I 2007 & Supp. II 2008)) (inserting a provision establishing a National Operations Center in Title V of the Homeland Security Act of 2002). For example, H.R. 4840 required the director of FEMA to have experience in the field of crisis management. H.R. 4840, 109th Cong. § 2(a)(1) (2006) (requiring the director to be an individual who possesses "demonstrated ability in, knowledge of, and extensive background in emergency or disaster-related management"). Similarly, PKEMRA requires administrators to have "a demonstrated ability in and knowledge of emergency management and homeland security." Post Katrina Emergency Management Reform Act of 2006, tit. V, § 503(c)(2)(A), 120 Stat. at 1397 (codified as amended at 6 U.S.C. §§ 311–21m, 701). For details on the proposals to remove FEMA from DHS, see generally Press Release, CHS, Thompson, King, Reichert, and Pascrell Call for Keeping FEMA in the Department of Homeland Security (Apr. 12, 2006), *available at* http://hsc.house.gov/press/index.asp?ID=38&SubSection=1&Issue=0&DocumentType=0&PublishDate=0 ("Removing FEMA from DHS would only exacerbate the agency's problems. It would reduce FEMA's access to the vast resources available within the Department, create duplicative response efforts for natural and manmade disasters and significantly delay our ability to prepare for future emergencies"). Representative James L. Oberstar (D-Minn.), Chairman of T&I, has led efforts in Congress to reinstate FEMA as an independent cabinet-level agency reporting to the President. *See* Memorandum from James Oberstar to President-Elect Barack Obama (Dec. 17, 2008), *available at* http://homeland.cq.com/hs/flatfiles/temporaryItems/20081218FEMAletter.pdf.

[189] Upon introduction, H.R. 1 was referred to CHS and was additionally referred to the Committees on Energy and Commerce, Judiciary, Intelligence (Permanent Select), Foreign Affairs, T&I, Oversight and Government Reform, and Ways and Means. The Library of Con-

9/11 Act, with a specific requirement that at least twenty-five percent of a state's SHSGP and UASI funds be dedicated towards law enforcement terrorism prevention activities.[192] Recognizing that terrorism preparedness and natural disaster preparedness are not mutually exclusive, CHS also specifically stated that states were not prohibited from using grant funds "in a manner that enhances preparedness for disasters unrelated to acts of terrorism, if such use assists such governments in achieving target capabilities related to preventing, preparing for, protecting against, or responding to acts of terrorism."[193]

Support from across America after September 11th and Katrina demonstrated the power of the citizenry; this power needs to be better organized and utilized by FEMA. For example, CHS ushered a DHS authorization bill through the House in 2007[194] which included a specific authorization for DHS to engage the Citizen Corps program to promote volunteerism and to help train citizens in emergency preparedness.[195] Similarly, the author cosponsored The Citizen and Community Preparedness Act of 2008, which authorized a more robust Citizen Corps program at DHS.[196] The author also introduced a related concept in the Homeland Security Relief Corps Act of 2008, which brought citizens together to assist in recovery and rebuilding efforts, particularly along the Gulf Coast region.[197] These bills describe the actions that are necessary to take advantage of the citizenry's commitment to securing the nation.

As long as communities exist near coasts, along fault lines, and exposed to other forces of nature, there will continue to be emergencies, crises, disasters, and catastrophes. In areas of the country that often witness the brute force of nature, there is a responsibility to be prepared, respond effectively, aid in recovery, and mitigate potential dangers, particularly when it comes to low-income communities without the resources to protect themselves. Because uprooting communities, livelihoods, and history is not always a feasible option, the country must better prepare its cities for inevitable natural disasters that will occur.

---

gress, H.R. 1: All Actions, http://www.thomas.gov/cgi-bin/bdquery/z?d110:HR00001:@@@X (last visited Apr. 13, 2010).

[190] SHSGP provides funds to assist state, local, and tribal governments in preventing, preparing for, protecting against, and responding to acts of terrorism. *See* Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, tit. I, § 101, sec. 2004, 121 Stat. 266, 277–79 (codified at 6 U.S.C. § 605 (Supp. I 2007)) (adding section 2004 to the Homeland Security Act).

[191] UASI provides grants to assist high-risk urban areas in preventing, preparing for, protecting against, and responding to acts of terrorism. *Id.* § 101, sec. 2003, 121 Stat. at 274–77 (codified at 6 U.S.C. § 604) (adding section 2003 to the Homeland Security Act).

[192] § 101, secs. 2003–04.

[193] *Id.*; *see also* 6 U.S.C. § 609(c).

[194] H.R. 1684, 110 Cong. (2007).

[195] *Id.* § 1111.

[196] H.R. 5890, 110th Cong. (2008) (formally authorizing the Citizen Corps Program and providing it with the necessary funding to be effective).

[197] H.R. 6425, 110th Cong. (2008).

V. Border Security

CHS has been charged with jurisdiction over DHS's border security functions.[198] Achieving meaningful border security poses many challenges. It requires significant resources and personnel, a commitment to using existing resources more effectively, and efficient technology solutions. Perhaps just as importantly, it necessitates overcoming political and jurisdictional concerns that have long impeded progress in this vital area. The following Sections offer a brief history of border security in the United States, examine the essential elements of border security and the obstacles to achieving it, and conclude with border security proposals and challenges associated with enacting legislation that addresses border security concerns.

A. Background

1. History of Border Protection

In the 19th century, Congress began enacting legislation restricting immigration to the United States.[199] In 1924, Congress established the U.S. Border Patrol to prevent aliens, contraband, and alcohol from crossing our nation's borders.[200] By the 1990s, the U.S. government began to construct physical barriers along the southwestern border to prevent the unauthorized entry of people and goods.[201] Since that time, Congress has regularly enacted legislation to further define procedures for entering our country.[202] However, only after the terrorist attacks of 2001 did Congress begin to view border control as a matter of national security.

With the passage of the Homeland Security Act of 2002,[203] a new DHS Directorate of Border and Transportation Security ("BTS") was charged with securing the nation's borders, waters, and transportation systems.[204] Fur-

---

[198] *See* House Rules, *supra* note 25, at X.1(i)(3)(A).

[199] *See* Law of May 6, 1882, 22 Stat. 58 (repealed 1943) (Chinese Exclusion); Law of March 3, 1875, 18 Stat. 477 (repealed 1974) (Page Act).

[200] Department of Labor Appropriation Act of 1924, Pub. L. No. 68-153, 43 Stat. 205, 240.

[201] CBP.gov, 85 Years of Protected By, http://cbp.gov/xp/cgov/border_security/border_patrol/85th_anniversary.xml (last visited Apr. 14, 2010)

[202] *See* Implementing Recommendations of the 9/11 Commission Act of 2007, tit. VII, 121 Stat. 266, 338–51 (codified as amended in scattered sections of 6, 8 U.S.C.); Real ID Act of 2005, Pub. L. No. 109-13, 119 Stat. 302 (codified as amended in scattered sections of 8 U.S.C.); Enhanced Border Security and Visa Entry Reform Act of 2002, Pub. L. No. 107-173, 116 Stat. 543 (codified as amended in scattered sections of 8 U.S.C.).

[203] Pub. L. No. 107-296, 116 Stat. 2135 (codified as amended in scattered sections of 6 U.S.C.).

[204] *Id.* at §§ 401-402, 116 Stat. at 2177-78; *see also* Jennifer E. Lake, Cong. Research Serv., Department of Homeland Security: Consolidation of Border and Transportation Security Agencies (2003).

ther, pursuant to section 872 of the Homeland Security Act of 2002,[205] President George W. Bush modified his original DHS reorganization plan to establish a Bureau of Customs and Border Protection and a Bureau of Immigration and Customs Enforcement within BTS.[206]

Today, U.S. Customs and Border Protection ("CBP") and Immigration and Customs Enforcement ("ICE") remain the two DHS components primarily responsible for border security. CBP's primary mission is keeping terrorists and terrorist weapons out of the country while facilitating legitimate trade and travel.[207] CBP's Office of Field Operations is charged with protecting America's borders at official points of entry ("POEs"), while the Office of Border Patrol is tasked with preventing illegal entry into the United States of people and contraband between the POEs.[208] CBP's Office of Air and Marine is charged with patrolling the nation's land and sea borders via air and watercraft to stop terrorists, drug smugglers, and undocumented aliens before they enter the United States.[209]

ICE consolidated the investigative and enforcement functions of the former Immigration and Naturalization Service ("INS") and the Customs Service.[210] ICE's mission is to detect and prevent terrorist and criminal acts by targeting the people, money, and materials that support terrorist and criminal networks.[211] As such, ICE is an important component of our nation's border security network, even though much of its focus is on enforcement in the interior of the United States.

2. Defining the Border

Mention of "the border" often conjures up images of dusty towns and remote stretches of desert running along the Rio Grande in the American Southwest.[212] In reality, 327 official POEs and thousands of miles of land perimeter and coastline comprise the borders of the United States.[213] In fiscal

---

[205] Homeland Security Act of 2002, Pub. L. No. 107-296, § 872, 116 Stat. at 2243 (codified at 6 U.S.C. § 452 (2006)).

[206] *See generally* Press Release, DHS, Border Reorganization Fact Sheet (May 10, 2010), *available at* http://www.dhs.gov/xnews/releases/press_release_0073.shtm.

[207] CBP.gov, Protecting Our Borders Against Terrorism, http://cbp.customs.gov/xp/cgov/about/mission/cbp.xml (last visited Apr. 14, 2010).

[208] CBP.gov, This is CBP, http://www.cbp.gov/xp/cgov/about/mission/cbp_is.xml (last visited Apr. 14, 2010).

[209] *Id.*

[210] *See* Press Release, DHS, Border Reorganization Fact Sheet (Jan. 30, 2003), *available at* http://www.dhs.gov/xnews/releases/press_release_0073.shtm.

[211] ICE, About U.S. Immigration and Customs Enforcement, http://www.ice.gov/about/index.htm (last visited Apr. 14, 2010).

[212] *See, e.g.*, Walter Nugent, *Where is the American West? Report on a Survey*, MONT.: MAG. W. HIST., Summer 1992, at 11 (reporting on results of a survey in which people characterized the west using "geographical definitions such as aridity, scenery, open space, lack of population density, or environment").

[213] CBP.gov, Securing America's Borders, http://cbp.gov/xp/cgov/border_security/bs/border_sec_initiatives_lp.xml (last visited Feb. 6, 2010).

year 2009, 361.2 million travelers and more than 108.5 million cars, trucks, buses, trains, vessels, and aircraft entered the United States, and more than 556,000 individuals were apprehended at and between POEs.[214] Taken together, these numbers indicate the immense size and scope of the border security challenge facing DHS and policymakers in Congress.

The U.S.-Mexico border region stretches approximately two thousand miles across California, Arizona, New Mexico, and Texas.[215] It encompasses major metropolitan areas like San Diego, cities with military installations and large federal law enforcement presences, such as El Paso, numerous smaller, mostly agricultural communities, and vast areas like Big Bend National Park. This varied nature of the region contributes to the challenge of securing the border.

At the same time, the U.S.-Canada border is often overlooked as a potential security threat. Our northern border spans over four thousand miles and twelve states.[216] Like the southwestern border, the region is varied, with major border crossings near Seattle, Detroit, and Buffalo, as well as small towns, densely forested areas, and wide-open prairies. Historically, the U.S.-Canada border has been touted as the longest open border in the world, which speaks to the cooperative relationship long enjoyed by the two countries.[217] After September 11, however, the wisdom of leaving America's northern border relatively open is not certain.

In addition to the land borders, the United States also has thousands of miles of maritime border, which includes seaports and open coastline.[218] Unlike the land borders, where those who enter or attempt to enter between the POEs are generally engaged in illicit activity, vessels engaged in legitimate commercial or recreational activity may intermingle with those engaged in illicit activity in the maritime environment.[219] Therefore, identifying and interdicting those engaged in illicit activity in this environment poses a unique border security challenge.

---

[214] Press Release, CBP, CBP FY09 Data Shows Significant Success in Securing Borders, Facilitating Travel and Trade (Nov. 24, 2009), *available at* http://www.cbp.gov/xp/cgov/newsroom/news_releases/archives/2009_news_releases/nov_09/11242009_8.xml.

[215] BLAS NUÑEZ-NETO, CONG. RESEARCH SERV., BORDER SECURITY: THE ROLE OF THE U.S. BORDER PATROL 2 (2005).

[216] *Id.*

[217] *See* Hillary Rodham Clinton, U.S. Sec'y of State, Remarks at the 100th Anniversary of the Boundary Waters Treaty (June 13, 2009), *available at* http://www.state.gov/secretary/rm/2009a/06/124716.htm.

[218] U.S. COAST GUARD, MARITIME STRATEGY FOR HOMELAND SECURITY 7 (2002), *available at* http://www.uscg.mil/History/articles/uscgmaritimestrategy2002.pdf (noting that DHS is responsible for protecting a border including 95,000 miles of shoreline, a 3.4 million square mile exclusive economic zone, and 350 official ports of entry).

[219] JAYETTA Z. HECKER, GAO, GAO-02-993T, PORT SECURITY: NATION FACES FORMIDABLE CHALLENGES IN MAKING NEW INITIATIVES SUCCESSFUL 3 (2002) (stating that "[d]rugs and illegal aliens are routinely smuggled into this country, not only in small boats but also hidden among otherwise legitimate cargoes on large commercial ships" and noting that "these same pathways are available for exploitation by a terrorist organization or any nation or person wishing to attack us surreptitiously").

Finally, America's international airports are considered the functional equivalent of borders.[220] As such, CBP is charged with vetting air passengers prior to their departure for the United States and once they arrive at airports in the United States.[221] As in the maritime environment, the challenge for DHS is to identify potential security threats in the flow of legitimate travelers—a challenge clearly illustrated by the failure to stop Umar Farouk Abdulmutallab, who allegedly attempted to detonate an explosive device on a flight bound from Amsterdam to Detroit on Christmas Day in 2009.[222]

B. Elements of Border Security

DHS officials frequently refer to the "three-legged stool" of border security: personnel, infrastructure, and technology.[223] The appropriate mix of these resources is essential to achieving border security. Adequate personnel are integral to operating POEs, patrolling areas between the POEs, and investigating border-related criminal activity. Likewise, appropriate infrastructure, including inspection areas at POEs and fencing and vehicle barriers between the POEs, is an important tool for border management. Finally, given the scope of the challenge, technology is an essential force-multiplier in the effort to secure the borders. While there may be general agreement about the essential elements of border security, there is often disagreement about which of the three legs should be a priority.

1. Personnel

Since September 11, many have focused on increasing the number of border security personnel, particularly the number of Border Patrol agents

---

[220] Almeida-Sanchez v. United States, 413 U.S. 266, 272–73 (1973); United States v. Hill, 939 F.2d 934, 936 (11th Cir. 1991); United States v. Gaviria, 805 F.2d 1108, 1112 (2d Cir. 1986).

[221] *See generally* GAO, GAO-08-219, BORDER SECURITY: DESPITE PROGRESS, WEAKNESSES IN TRAVELER INSPECTIONS EXIST AT OUR NATION'S PORTS OF ENTRY 10 (2007) [hereinafter BORDER SECURITY: DESPITE PROGRESS] (describing CBP's responsibilities with respect to screening passengers and goods as they enter the country).

[222] *See* Michael Leahy & Spencer S. Hsu, *Nigerian Arrested in Failed Jet Attack*, WASH. POST, Dec. 26, 2009, at A1.

[223] *See, e.g.*, *The FY 2010 Budget for Immigration and Customs Enforcement, Customs and Border Protection, and the U.S. Coast Guard: Hearing Before the Subcomm. on Border, Maritime and Global Counterterrorism of the H. Comm. on Homeland Sec.*, 111th Cong. (2009) [hereinafter *FY 2010 Budget Hearing*] (testimony of Jayson Ahern, Acting Comm'r, CBP, DHS), *available at* http://homeland.house.gov/SiteDocuments/20090611103714-74925.pdf (explaining CBP's strategy for establishing "operational control . . . as [a] 'three legged stool'"); *see also The Secure Border Initiative: SBInet Three Years Later: Hearing Before the Subcomm. on Border, Maritime and Global Counterterrorism of the H. Comm. on Homeland Sec.*, 111th Cong. (2009) [hereinafter *SBInet Hearing*] (testimony of David Aguilar, Chief, U.S. Border Patrol), *available at* http://homeland.house.gov/SiteDocuments/20090917103631-30364.pdf (explaining CBP's strategy for establishing "operational control . . . as [a] 'three legged stool'").

who are responsible for patrolling the border between the POEs.[224] President George W. Bush pledged to double the number of Border Patrol agents during his term in office from approximately 9000 agents to about 18,000 agents.[225] With funding from Congress, DHS achieved that goal.[226]

While DHS has had success in expanding the ranks of the Border Patrol, there has been far less progress toward hiring additional CBP officers for the land, sea, and air POEs. Since the end of fiscal year 2004, DHS has added less than 2000 new CBP Officers for land, air, and seaports combined.[227] In that same period of time, the Department added almost three times as many new Border Patrol agents for monitoring between the POEs.[228] As a whole, the CBP workforce increased 10% during 2009.[229] While the number of CBP officers increased by 7% to a total of 21,294, Border Patrol agent staffing increased by 15%, from 17,499 in fiscal year 2008 to 20,119 at the end of fiscal year 2009.[230]

CBP has declined to confirm whether it is understaffed at the POEs.[231] However, the National Treasury Employees Union, which represents CBP

---

[224] Congress has been very concerned with the number of personnel patrolling our northern and southern borders and has acted on numerous occasions, providing funding to ensure that our borders are sufficiently protected. *See, e.g.*, LISA M. SEGHETTI, CONGRESSIONAL RESEARCH SERVICE, BORDER SECURITY: U.S.-CANADA IMMIGRATION BORDER ISSUES 2–3 (2004), http://www.ndu.edu/library/docs/crs/crs_rs21258_28dec04.pdf (noting that Congress authorized funding for additional border patrol personnel in acts including the PATRIOT Act, the Enhanced Border Security and Visa Entry Reform Act of 2002 and the Intelligence Reform and Terrorism Prevention Act of 2004).

[225] *See* Press Release, Office of the White House Press Sec'y, President Bush Signs Department of Homeland Security Appropriations Act (Oct. 4, 2006), *available at* http://georgewbush-whitehouse.archives.gov/news/releases/2006/10/20061004-2.html.

[226] *See* Press Release, CBP, Securing America's Borders: CBP Fiscal Year 2009 in Review Fact Sheet (Nov. 24, 2009), *available at* http://www.cbp.gov/xp/cgov/newsroom/news_releases/archives/2009_news_releases/nov_09/11242009_5.xml [hereinafter Press Release, Securing America's Borders] (noting that Office of Border Patrol met goal of hiring 6000 agents to employ more than 18,000 agents by the end of 2008).

[227] In fiscal year 2004, DHS employed 9509 CBP officers at non-border sites. DHS, CBP FULL TIME EMPLOYEE STATISTICS (2008) (chart attached to E-mail from Alison Northrop, Staff Dir., Subcomm. on Border, Maritime & Global Counterterrorism, CHS, to Stephanie Yablonski, DHS (Dec. 15, 2009, 11:22 AM EST) (on file with author) [hereinafter Agent E-mail from Northrop to Yablonski]). By the end of fiscal year 2009, DHS employed 11,433 CBP officers at non-border sites. DHS, CBP OFFICER AND AGRICULTURE SPECIALISTS FULL TIME PERMANENT EMPLOYEES ONLY FY08-FY09 (2009) (chart attached to E-mail from Stephanie Yablonski, DHS, to Alison Northrop, Staff Dir., Subcomm. on Border, Maritime & Global Counterterrorism, CHS (Dec. 15, 2009, 03:16 PM EST) (on file with author) [hereinafter Border E-mail from Yablonski to Northrop]).

[228] In fiscal year 2002, DHS employed 3971 border agents. *See* Agent E-mail from Northrop to Yablonski, *supra* note 227; *see also* Border E-mail from Yablonski to Northrop, *supra* note 227.

[229] Press Release, Securing America's Borders, *supra* note 226.

[230] *Id.*

[231] *Cargo Security at Land Ports of Entry: Are We Meeting the Challenge?: Hearing Before the Subcomm. on Border, Maritime, and Counterterrorism of the H. Comm. on Homeland Sec.*, 111th Cong. (2009) [hereinafter *Cargo Security Hearing*] (statement of Todd Owen, Executive Director, Cargo and Conveyance Security, Office of Field Operations, Customs and Border Protection), *available at* http://homeland.house.gov/SiteDocuments/20091022103904-48902.pdf.

officers, has indicated that it believes the position is understaffed by several thousand agents.[232] The number of new ICE Special Agents has also not kept pace with the growth in Border Patrol agents.[233] The consequences of understaffing at the POEs are potentially grave. A 2007 GAO report found serious security lapses at the POEs and concluded that thousands of individuals who should not have been allowed to enter the United States were admitted through land POEs in a single year.[234] CBP officers are overworked, frequently required to perform significant amounts of overtime, and unable to dedicate adequate time to training.[235] Both security and legitimate trade and travel suffer under these circumstances, generating concern among business, industry, and border community stakeholders.[236]

Clearly, the Border Patrol had been understaffed in the years prior to September 11.[237] But the reason behind faster growth of Border Patrol compared to CBP officers, ICE Special Agents, and other border security-related personnel is not clear. Perhaps, because Border Patrol agents apprehend hundreds of thousands of illegal aliens annually[238] in addition to protecting the nation from terrorists, their role in the hot-button immigration issue contributed to Congress's and the Bush administration's efforts to expand their ranks so remarkably.[239] Also, since the Border Patrol was moved to DHS intact from INS, while the CBP officer and ICE Special Agent positions were newly created, it is also possible that policymakers may have been more understanding of the mission of the Border Patrol.

Yet if Congress is truly interested in border security, not just immigration control, Congress and the Executive Branch must put a greater emphasis on providing the personnel necessary to fully staff all CBP positions, includ-

---

[232] *Id.* (statement of Colleen M. Kelley, National President, National Treasury Employees Union), *available at* http://homeland.house.gov/SiteDocuments/20091022103853-04230.pdf.

[233] E-mail from Chad Haddal, Analyst in Immigration Policy, Congressional Research Service, to Alison Northrop, Staff Dir., Subcomm. on Border, Maritime, and Global Counterterrorism, CHS (March 10, 2010, 08:59 EST) (on file with author).

[234] *Ensuring Homeland Security While Facilitating Legitimate Travel: The Challenge at America's Ports of Entry: Field Hearing Before the H. Comm. on Homeland Sec.*, 110th Cong. 20–22 (2008) (statement of Richard M. Stana, Director, Homeland Sec. and Justice Issues, GAO).

[235] *Id.* at 52 (2008) (statement of Colleen M. Kelley, National President, National Treasury Employees Union).

[236] *See generally id.*

[237] Sean Patrick Gallagher, ECONOMIC AND ADMINISTRATIVE IMPACT OF 9/11: WHY THE UNITED STATES BORDER WITH CANADA IS NO LONGER "UNDEFENDED" 4 (2005), *available at* http://insct.syr.edu/events&lectures/conferences/2005/GWOT_symposium/0Sean%20paper%20for%20website.pdf ("Pre September 11th, low volume border crossings were not adequately staffed 24 hours a day (meaning no agents would be on patrol and the border crossing essentially closed). The only thing preventing a terrorist from entering the country: a lone orange cone in the center of the road.").

[238] *See* NANCY RYTINA & JOHN SIMANSKI, DHS, FACT SHEET: APPREHENSIONS BY THE U.S. BORDER PATROL: 2005–2008 (2009), *available at* http://www.dhs.gov/xlibrary/assets/statistics/publications/ois_apprehensions_fs_2005-2008.pdf.

[239] *See generally* Blas Nuñez-Neto, Cong. Research Serv., Border Security: The Role of the U.S. Border Patrol (2008).

ing CBP officer positions for land, sea, and air, and ICE Special Agent positions related to border security.

2. Infrastructure

In order to discharge its duties, the Border Patrol deploys tactical infrastructure such as fencing and vehicle barriers.[240] Fencing prevents aliens from entering the country illegally, while vehicle barriers impede the entry of vehicles while still allowing for the entry of individuals.[241]

In 1990, the Border Patrol began erecting a barrier directly on the border to deter illegal entries in its San Diego Sector.[242] Completed in 1993, the San Diego primary fence covered the first fourteen miles of the border, starting at the Pacific Ocean.[243]

In 1996, Congress passed the Illegal Immigration Reform and Immigrant Responsibility Act ("IIRIRA"), which gave the Attorney General explicit authority to construct border fencing.[244] In 2005, Congress passed the REAL ID Act, which authorized the Secretary of Homeland Security to waive all legal requirements in order to expedite the construction of border fencing.[245] Then-Homeland Security Secretary Chertoff used the statutory waiver provided under the REAL ID Act a total of five times to circumvent myriad laws that were intended to protect the environment and to ensure public participation and input in the process.[246] In 2006, Congress passed the Secure Fence Act, which directed DHS to construct five separate stretches of fencing along the southern border, totaling 850 miles.[247] This requirement was modified by the Consolidated Appropriations Act of 2008, which authorized the Secretary to construct reinforced fencing along seven hundred

---

[240] *See* OFFICE OF BORDER PATROL & OFFICE OF POLICY & PLANNING, CBP, NATIONAL BORDER PATROL STRATEGY 15–16 (2004), *available at* http://www.cbp.gov/linkhandler/cgov/border_security/border_patrol/border_patrol_ohs/national_bp_strategy.ctt/national_bp_strategy.pdf.

[241] *See* CHAD C. HADDAL ET AL., CONG. RESEARCH SERV., BORDER SECURITY: BARRIERS ALONG THE U.S. INTERNATIONAL BORDER 1 (2009).

[242] *See id.*

[243] *Id.*

[244] Pub. L. No. 104-208, div. C, tit. I, subtit. A, § 102, 110 Stat. 3009, 3009-554 to -555 (1996) (codified as amended at 8 U.S.C. § 1103 (2006)).

[245] Pub. L. No. 109-13, div. B, tit. I, § 102, 119 Stat. 231, 306 (2005) (codified as amended at note following 8 U.S.C. § 1103 (Supp. I 2007)).

[246] *See* Notice of Determination, 73 Fed. Reg. 19,078 (Apr. 8, 2008) (determining it necessary to waive rules for specific project areas in California, Arizona, New Mexico, and Texas); Notice of Determination, 73 Fed. Reg. 18,294 (Apr. 4, 2008) (determining it necessary to waive rules for "project area" near Hidalgo County, Texas); Notice of Determination, 73 Fed. Reg. 18,293 (Apr. 3, 2008) (determining it necessary to waive rules for "project areas" in California, Arizona, New Mexico, and Texas); Notice of Determination, 72 Fed. Reg. 60,870 (Oct. 26, 2007) (determining it necessary to waive rules for area between Naco, Arizona and the San Pedro Riparian National Conservation Area); Notice of Determination, 72 Fed. Reg. 2535 (Jan. 19, 2007) (determining it necessary to waive rules for area surrounding the Barry M. Goldwater Range).

[247] Pub. L. No. 109-367, § 3, 120 Stat. 2638, 2368–39 (2006) (codified as amended at note following 8 U.S.C. § 1103).

miles of the southwest border, but also gave discretion to the Secretary over whether and where fencing was to be constructed.[248]

As of September 2009, there were 333.5 miles of pedestrian fence and 298.4 miles of vehicle fence in place along the southwestern border, for a total of 631.9 miles of tactical infrastructure.[249] Though CBP was scheduled to complete the remaining miles by November 2009, construction faces ongoing delays in a limited number of areas in part due to challenges in acquiring the necessary property rights from landowners.[250] Most of these challenges are in Texas because much of the border land there is privately owned (unlike in California, Arizona, and New Mexico, where the federal government owns or possesses an easement for land along the border).[251]

3. Technology

DHS, its components, and its federal partners utilize technology in a number of border security programs and initiatives. For example, foreign visitors have their biometrics entered into a database that tracks their travel to the United States, non-intrusive inspection equipment is used to scan the contents of cargo containers and trucks entering the country, and portal monitors check for radiological hazards as travelers and goods approach our POEs.[252] But perhaps the most-anticipated border security technology has been the development of a system to monitor the stretches of border between our nation's POEs.

The U.S. government has sought a technological solution to border security between ports of entry for almost fifteen years. The search for such a solution began in 1997 with the initial development of the Integrated Surveillance Intelligence System ("ISIS"), which was to consist of cameras, ground sensors, and an Intelligent Computer-Aided Detection system along

---

[248] Consolidated Appropriations Act of 2008, Pub. L. No. 110-161, div. E, tit. II, § 6, 121 Stat. 1844, 2047–48 (2007).

[249] *See* E-mail from Laura Cylke, Office of Cong. Affairs, CBP, to Alison Northrop, Staff Dir., Subcomm. on Border, Maritime, and Global Counterterrorism, CHS (Sept. 16, 2009, 03:19 EST) (on file with author) [hereinafter E-mail from Cylke to Northrop]; *see also* CBP, VEHICLE FENCE STATUS SHEET 9-4-09 (2009) (on file with author) (attached to E-mail from Cylke to Northrop, *supra*); CBP, PEDESTRIAN FENCE STATUS SHEET 9-4-09 (2009) (on file with author) (attached to E-mail from Cylke to Northrop, *supra*).

[250] *See, e.g.*, Defenders of Wildlife v. Chertoff, 527 F.Supp.2d 119 (D.D.C. 2007); County of El Paso v. Chertoff, No. EP-08-CA-196-FM, 2008 WL 4372693 (W.D. Tex. Aug. 29, 2008); *see also* Elana Schor, *Texans Sue Bush Administration Over Mexico Border Fence*, GUARDIAN (London), May 16, 2008, http://www.guardian.co.uk/world/2008/may/16/usa.immigration policy.

[251] In 1907, President Theodore Roosevelt reserved from appropriation "all public lands within sixty feet of the international boundary between the United States and the Republic of Mexico" in California, New Mexico, and Arizona. *See* Proclamation No. 758, 35 Stat. 2136 (May 27, 1907).

[252] *See* OFFICE OF FIELD OPERATIONS & OFFICE OF POLICY PLANNING, CBP, SECURING AMERICA'S BORDERS AT PORTS OF ENTRY: OFFICE OF FIELD OPERATIONS STRATEGIC PLAN FY 2007–2011 10–11 (2006), *available at* http://www.cbp.gov/linkhandler/cgov/border_security/port_activities/securing_ports/entry_points.ctt/entry_points.pdf.

the border.[253] However, ISIS was hampered by technological failures and ineffective management. After ten years and an expenditure of $239 million, the government ended the program.[254]

In 2004, DHS began developing the American Shield Initiative ("ASI") with the goal of maintaining and modernizing ISIS while expanding the technological capabilities of the program.[255] Like ISIS, ASI was intended to be a technology-based program with ground sensors, cameras, and manned control centers.[256] However, the Department abandoned ASI in 2005[257] without even seeking contractors to implement the program.[258]

On November 2, 2005, the Department announced the Secure Border Initiative ("SBI"), the third major attempt at developing a technological solution for securing America's borders.[259] SBI was planned as a multi-dimensional program to include additional border security personnel, such as Border Patrol agents, more tactical infrastructure, including pedestrian fencing and vehicle barriers, and increased detention capacity.[260] SBI also included a technology component called SBInet, which was launched in September 2006.[261] Like ISIS and ASI, SBInet is intended to create a "virtual fence" along the nation's borders using cameras, sensors, radar, and other equipment.[262]

In 2006, DHS awarded an Indefinite Delivery/Indefinite Quantity ("IDIQ") contract for the development of SBInet to a team led by Boeing Integrated Defense Systems.[263] According to that contract, an initial set of SBInet systems was to be deployed along the southwest border in early fiscal year 2009, and a full set of systems along the southwest and northern borders was to be completed later in the year.[264] However, as a result of a series of significant problems and delays, DHS does not plan to have tech-

---

[253] GAO, GAO-06-295, BORDER SECURITY: KEY UNRESOLVED ISSUES JUSTIFY REEVALUATION OF BORDER SURVEILLANCE TECHNOLOGY PROGRAM 1 (2006) [hereinafter GAO, BORDER SECURITY: KEY UNRESOLVED ISSUES].

[254] *Id.*

[255] *Id.*

[256] DHS, BUDGET-IN-BRIEF: FISCAL YEAR 2006, at 27 (2005), *available at* http://www.dhs.gov/xlibrary/assets/Budget_BIB-FY2006.pdf.

[257] *See generally* GAO, BORDER SECURITY: KEY UNRESOLVED ISSUES, *supra* note 253.

[258] *Id.* at 2, 39.

[259] *See* Press Release, DHS, Fact Sheet: Secure Border Initiative (Nov. 2, 2005), *available at* http://www.dhs.gov/xnews/releases/press_release_0794.shtm.

[260] *Id.*

[261] CBP, SBINET: SECURING U.S. BORDERS (2006), *available at* http://www.dhs.gov/xlibrary/assets/sbinetfactsheet.pdf.

[262] Randall C. Archibold, *28-Mile Virtual Fence is Rising Along the Border*, N.Y. TIMES, Jun. 26, 2007, http://www.nytimes.com/2007/06/26/us/26fence.html; *see also U.S. Puts Up Real Barriers to "Virtual Fence" Along Mexican Border*, PBS NEWSHOUR EXTRA, Apr. 2, 2010, http://www.pbs.org/newshour/extra/features/us/jan-june10/fence_04-02.html.

[263] Press Release, Boeing, Boeing Team Awarded SBInet Contract by Department of Homeland Security (Sept. 21, 2006), *available at* http://www.boeing.com/news/releases/2006/q3/060921a_nr.html.

[264] *See* GAO, SECURE BORDER INITIATIVE: DELAYS, *supra* note 15, at 11.

nology-based barriers deployed along the southern border until 2016.[265] The date for deployment along the northern border is even more uncertain.[266] Yet, despite these setbacks, SBI's funding amounted to over $3.7 billion from fiscal year 2005 to fiscal year 2009.[267] In early 2010, Secretary Napolitano announced DHS would review the program and that funds for the program would be frozen until that assessment is completed.[268] However, despite the freeze, DHS received an additional $800 million for the program for fiscal year 2010.[269]

C. The Fence

As noted above, Congress and the Executive have provided significant resources for constructing fencing along the southwestern border. Unfortunately, construction costs have risen significantly above initial estimates, and questions about the efficacy of the fence persist.

According to GAO, for fencing completed as of October 31, 2008, the per mile cost of fencing averaged $3.9 million for pedestrian fencing and $1 million for vehicle fencing.[270] However, the average per mile cost of fencing increased after contracts were awarded, to $6.5 million per mile for pedestrian fencing and $1.8 million per mile for vehicle fencing.[271] Officials have indicated that costs rose due to factors such as property acquisition expenses, rising costs of labor and materials, and added expenses from the compressed construction timeline.[272]

According to GAO, total life-cycle costs for all tactical infrastructure constructed to date, including pre-SBI infrastructure as well as that planned for fiscal years 2009, 2010, and 2011, are estimated at about $6.5 billion.[273] The lifecycle cost estimates include deployment, operations, and future maintenance costs for all tactical infrastructure, including the fence, roads, and lighting.[274] CBP has estimated the lifespan of the fence to be approximately twenty years and plans to allocate $75 million for fence operations

---

[265] *SBInet Hearing*, *supra* note 223 (statement of Richard M. Stana, Director, Homeland Security and Justice Issues, GAO) (reprinted in GAO, GAO-09-1013T, SECURE BORDER INITIATIVE: TECHNOLOGY DEPLOYMENT DELAYS PERSIST AND THE IMPACT OF BORDER FENCING HAS NOT BEEN ASSESSED 3 (2009) [hereinafter STANA SBINET TESTIMONY]).

[266] *Id.*

[267] *Id.*

[268] Press Release, DHS, Statement by Homeland Security Secretary Janet Napolitano (Mar. 16, 2010), *available at* http://www.dhs.gov/ynews/releases/pr_1268769368466.shtm.

[269] Department of Homeland Security Appropriations Act of 2010, Pub. L. No. 111-83, 123 Stat. 2145.

[270] *See* GAO, SECURE BORDER INITIATIVE: DELAYS, *supra* note 15, at 21.

[271] *Id.*

[272] *Id.*

[273] *SBInet Hearing*, *supra* note 223 (statement of Richard M. Stana, Director, Homeland Security and Justice Issues, GAO) (reprinted in STANA SBINET TESTIMONY, *supra* note 265, at 5).

[274] *Id.*

and maintenance in fiscal year 2009 and again in 2010.[275] A significant use of the operations and maintenance funding is to repair breaches in the fence. According to CBP data, there had been 3363 breaches in the fence as of May 14, 2009, and the repair costs of each breach averaged $1300.[276]

According to CBP, "tactical infrastructure, coupled with additional trained Border Patrol agents, had increased the miles of the southwest border under effective control."[277] GAO explains that:

> DHS defines effective control of the U.S. borders as the ability to consistently (1) detect illegal entries into the United States between the ports of entry, (2) identify and classify these entries to determine the level of threat involved, (3) effectively respond to these entries, and (4) bring events to a satisfactory law enforcement resolution.[278]

As of May 31, 2009, CBP determined that 894 miles of border are under effective control, including 697 miles along the southwestern border, 32 along the northern border, and 165 in the coastal regions.[279]

However, despite a $2.4 billion investment, GAO found that CBP cannot account separately for the impact of tactical infrastructure on gains or losses in the level of effective border control.[280] Currently, the performance of tactical infrastructure is measured simply by miles constructed, which does not reveal a program's discrete contribution to effective border control.[281] Until DHS determines the contribution of tactical infrastructure to border security, Congress, GAO, DHS, and other stakeholders will be unable to assess whether this significant investment was justified, or whether there would have been a better use of our limited border security enforcement resources.

Border security fencing is necessary where it makes sense, such as in certain limited areas where it is integral to the Border Patrol's enforcement efforts.[282] But there are at least two factors that suggest recent border fencing is sometimes not the best border security solution. First, despite invocations of the terrorist threat to justify building the fence,[283] there is no evidence that

---

[275] *See* GAO, SECURE BORDER INITIATIVE: DELAYS, *supra* note 15, at 21.

[276] *Id.* at 23.

[277] *Id.* at 25.

[278] *Id.*

[279] *See, e.g.*, *FY 2010 Budget Hearing*, *supra* note 223 (statement of Jayson Ahern, Acting Comm'r, CBP, DHS).

[280] GAO, SECURE BORDER INITIATIVE: DELAYS, *supra* note 15, at 6.

[281] *Id.* at 26.

[282] *See Border Security: Infrastructure, Technology, and the Human Element: Hearing Before the Subcomm. on Border, Maritime, and Global Counterterrorism of the H. Comm. on Homeland Sec.*, 110th Cong. 28-29 (2007) (statement of David Aguilar, Chief, Office of Border Control, CBP, DHS) (discussing the need for fencing, particularly in urban areas).

[283] *See* 152 CONG. REC. H6537, H6582–84 (daily ed. Sept. 14, 2006) (statements of Reps. Peter King (R-N.Y.) and David Dreier (R-Cal.)) (speaking in support during the House's debate on H.R. 6061, the Secure Fence Act of 2006). The Act also includes "entries by ter-

terrorists have attempted to cross the southwestern border.[284] Second, the amount of fencing and the locations for fence construction set forth in the Secure Fence Act were mandated by Congress rather than determined by administrative agencies with expertise on the issue.[285] While the fence may have been good politics, the question of whether it was good policy for national security remains unanswered.

D. Terrorist Threats at the Border

The possibility of terrorists or their weapons entering the United States poses a significant threat to our border security. This includes individuals who enter the country surreptitiously between the POEs as well as those who might come to the United States legally. For example, the so-called "Millennium Bomber," Ahmed Ressam, arrived via a ferry from Canada and was interdicted at a POE with explosives intended to blow up Los Angeles International Airport,[286] and the September 11 hijackers entered the United States on visas.[287] Similarly, the Christmas Day bomber, Umar Farouk Abdulmutallab, was a Nigerian traveling on a U.S. visa.[288]

While we know terrorists have attempted to enter the United States via our northern border and by air, to date there is no evidence that they have done so via our southwestern border.[289] Nevertheless, the overwhelming majority of our border security personnel, infrastructure, and technology resources continue to be directed to the U.S.-Mexico border. Fewer than ten percent of Border Patrol agents are assigned to the U.S.-Canada border.[290]

---

rorists" in its definition of "operational control" of the border, which the Secretary is required to achieve within eighteen months of enactment. 8 U.S.C. § 1701 note (2006).

[284] *See* Matthew B. Stannard, *While Security Fears Stoke Support for Barrier, Wall's Merits for War on Terror are Debatable*, S.F. CHRON., Feb. 26, 2006, http://articles.sfgate.com/2006-02-26/news/17281478_1_cross-border-terrorist-groups-threat (noting that, according to experts, no individuals known to have committed or attempted terrorist acts on U.S. soil entered the United States across the Mexican border).

[285] Secure Fence Act of 2006, Pub. L. No. 109-367, § 3, 120 Stat. 2638, 2639 (codified as amended at note following 8 U.S.C. § 1103 (Supp. I 2007)) (defining the areas of land on which the Secretary of Homeland Security is directed to construct a border fence). While the Consolidated Appropriations Act of 2008 amended the Secure Fence Act of 2006 by removing the specific locations where the border fence must be built, the Act still defined the minimum length of the fence rather than leaving it to the discretion of the Secretary. *See* Consolidated Appropriations Act of 2008, Pub. L. No. 110-161, div. E, tit. V, § 564(a)(2)(B)(ii), 121 Stat. 1844, 2090–91 (2007) (codified at note following 8 U.S.C. § 1103).

[286] *See generally* Eric Lichtblau, *U.S. Airports to Tighten Security Over Terror Fears*, L.A. TIMES, Dec. 22, 1999, at 1 (describing how Ahmed Rassan "crossed on a ferry from Canada with more than 130 pounds of bomb-making chemicals hidden in the trunk of his car, as well as 4 homemade timing devices apparently designed to detonate bombs").

[287] *See* 9/11 COMMISSION REPORT, *supra* note 23, at 215–17 (describing Nawaf al Hamzi and Khalid al Mihdhar's entry into the United States and explaining that they were only qualified to participate in the 9/11 plot because of their ability to get valid U.S. visas); *id*. at 225–26 (describing how 9/11 hijacker Hani Hanjour entered the United States on a valid student visa).

[288] Leahy & Hsu, *supra* note 222.

[289] *See generally National Security Threats Hearing*, *supra* note 9.

[290] BLAS NUÑEZ-NETO, BORDER SECURITY, *supra* note 215, at 19.

Similarly, there are significantly more CBP officers assigned to the southwestern border than the northern border.[291] Hundreds of miles of border fencing have also been constructed on the southwestern border, while there is no fencing on the northern border.[292]

While this allocation of resources may make sense for combating illegal immigration, it does not make sense from a border security perspective. If our primary objective truly is security, we must make an honest, comprehensive assessment of all the potential threats at our nation's borders and allocate resources accordingly.

E. Shortcomings

1. Ports of Entry

CBP has the dual mission of regulating the entry of travelers and goods to the United States, while also facilitating the flow of legitimate trade and travelers.[293] At POEs, CBP officers screen for possible threats, determine individuals' eligibility to enter the country, and collect taxes, duties, and fees.[294] ICE then investigates criminal organizations that take advantage of weaknesses in legitimate trade, travel, and financial systems.[295] ICE special agents, situated at or near the POEs, as well as throughout the interior, work to detect, disrupt, and dismantle cross-border criminal networks engaged in the smuggling of people, narcotics, bulk cash, and weapons across borders.[296] In the event of an interdiction of people or a seizure of narcotics, bulk cash, or weapons at a POE, ICE responds to CBP's notification and conducts interviews and other investigative activities related to the incident.[297]

For a November 2007 report, GAO visited several air and land POEs to identify strengths and weaknesses in operations.[298] The report indicates that

---

[291] In fiscal year 2009, for example, out of 21,058 CBP officers, 9625 officers were assigned to a U.S. border. Of those officers, 5660 CBP officers, or almost 60% of the officers assigned to a border, were assigned to the southern border. In contrast, only 3965 CBP officers were assigned to the northern border. *See* Border E-Mail from Yablonski to Northrop, *supra* note 227; *see also* DHS, CHART—CBP OFFICER AND AGRICULTURE SPECIALISTS FULL TIME PERMANENT EMPLOYEE STATISTICS FY 08–FY 09 (2009) (on file with author) (attached to Border E-mail from Yablonski to Northrop, *supra* note 227).

[292] HADDAL ET AL., *supra* note 241 (describing the status of fencing along the U.S. southern border and the options available for the northern border).

[293] *See* GAO, SECURE BORDER INITIATIVE: DELAYS, *supra* note 15, at 1 n.1.

[294] *See* SECURING AMERICA'S BORDERS AT PORTS OF ENTRY, *supra* note 252, at ii.

[295] *FY 2010 Budget Hearing*, *supra* note 223 (statement of John T. Morton, Assistant Secretary, ICE), *available at* http://homeland.house.gov/SiteDocuments/20090611103730-30370.pdf.

[296] *See id.*

[297] *Cargo Security Hearing*, *supra* note 231 (statement of Janice Ayala, Deputy Assistant Dir., Office of Investigations, DHS), *available at* http://homeland.house.gov/SiteDocuments/20091022103845-45935.pdf.

[298] *See* BORDER SECURITY: DESPITE PROGRESS, *supra* note 221.

POEs have had a number of problems, including weakness in traveler inspection procedures, deficiencies in physical infrastructure, staffing shortages, and poor training.[299] Furthermore, increased efforts to secure American borders between the POEs through additional Border Patrol agents, fencing, and technology may actually cause individuals to attempt to enter or bring goods into the country illegally through the POEs instead.[300]

While congestion at POEs has increased over the years, infrastructure has not kept pace with need. The American Recovery and Reinvestment Act of 2009 provided $420 million for the planning, management, design, alteration, and construction of CBP-owned border POEs and $300 million for POEs owned by the General Services Administration.[301] This investment was long overdue, but affects only a limited number of POEs. Additional investments will be necessary to fully modernize our nation's POEs to meet security and facilitation-related demands.

2. Entry-Exit System

According to the 9/11 Commission Report, "[c]ompleting a biometrics-based entry-exit system is an essential investment in our national security."[302] In recognition of this problem, DHS revamped the entry-exit system that had first been mandated by IIRIRA[303] and renamed it US-VISIT in 2003.[304] DHS has completed implementing the biometric entry portion of US-VISIT, under which travelers' fingerprints and photographs are collected upon entry to the United States.[305] However, DHS has yet to implement an operational biometric exit system to track travelers' departure from the country.[306]

US-VISIT exit procedures were initially piloted through exit kiosks at twelve airports and two seaports, but DHS terminated the exit pilot programs on May 6, 2007.[307] In its examination of the pilot programs, GAO reported

---

[299] *See generally id.*

[300] *See* HADDAL ET AL., *supra* note 241, at 33–34 (discussing the unintended consequences of border fencing including changing the migration patterns of illegal immigrants).

[301] *See generally* American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115.

[302] *See* 9/11 COMMISSION REPORT, *supra* note 23, at 389.

[303] Pub. L. No. 104-208, § 110, 110 Stat. 3009-546, 3009-558–59 (1996) (codified as amended at 8 U.S.C. § 1365a (2006)).

[304] *See* LISA M. SEGHETTI & STEPHEN R. VIÑA, CONG. RESEARCH SERV., U.S. VISITOR AND IMMIGRANT STATUS INDICATOR TECHNOLOGY 1 (2005). The goal of US-VISIT is and has been to track the entry and exit of every foreign national that enters the United States. *Id.*

[305] DHS, US-VISIT, http://www.dhs.gov/files/programs/usv.shtm (last visited Apr. 27, 2010).

[306] CHS, AMERICA'S UNFINISHED WELCOME MAT: US-VISIT A DECADE LATER 2 (2007), *available at* http://homeland.house.gov/SiteDocuments/20070628115232-48709.pdf (noting that in February 2007, the US-VISIT Program Office "acknowledged that a biometric exit capability could not be implemented at land POEs without incurring costly impacts, and that a feasible solution . . . may not be available for another 5 to 10 years").

[307] MAJORITY STAFF OF H. COMM. ON HOMELAND SEC., AMERICA'S UNFINISHED WELCOME MAT: US-VISIT A DECADE LATER 6 (2007), *available at* http://homeland.house.gov/

low compliance rates, poor planning, and inadequate evaluations.[308] In 2008, DHS issued a Notice for Proposed Rulemaking ("NPRM") for a new US-VISIT air exit system that would require the airlines to collect foreign travelers' biometrics.[309] The NPRM contained a number of alternatives, including a kiosk option,[310] but DHS ultimately chose an option requiring the airlines to collect the biometrics.[311] This decision drew sharp criticism from the air carriers, who objected to the potential costs.[312] Members of CHS also expressed opposition to the proposal because it would delegate border security and immigration responsibilities—inherently governmental functions[313]—to the airlines.[314]

Most recently, in the summer of 2009, DHS piloted two government-operated US-VISIT exit solutions, partly in response to congressional pressure.[315] One involved CBP officers collecting travelers' fingerprints at the departure gate, while the other had Transportation Security Administration personnel taking biometrics at the security checkpoint.[316] DHS is expected to promulgate another final rule governing the operation of US-VISIT in fiscal year 2010.[317]

Thus, an entry-exit system to track foreign travel to the United States remains incomplete. GAO has concluded that the longer DHS goes without an exit-tracking capability, the more its ability to effectively and efficiently

---

SiteDocuments/20070628124229-93571.pdf (noting that DHS terminated the US-VISIT exit pilots on May 6, 2007).

[308] *See generally* BORDER SECURITY: DESPITE PROGRESS, *supra* note 221.

[309] Collection of Alien Biometric Data Upon Exit From the United States at Air and Sea Ports of Departure, 73 Fed. Reg. 22,065 (Apr. 24, 2008) (to be codified in scattered sections of 8, 19 C.F.R.).

[310] *Id.* at 22,077.

[311] *Id.* at 22,072.

[312] *See, e.g.*, *US-VISIT Exit: Closing Gaps in Our Security: Hearing Before the Subcomm. on Border, Maritime and Global Counterterrorism of the H. Comm. on Homeland Sec.*, 110th Cong. 35–37 (2007) (statement of James C. May, President and Chief Executive Officer, Air Transport Association).

[313] At its core, "[a]n 'inherently governmental function' is one that, as a matter of law and policy, must be performed by federal government employees and cannot be contracted out because it is 'intimately related to the public interest.'" JOHN R. LUCKEY ET AL., INHERENTLY GOVERNMENTAL FUNCTIONS AND DEPARTMENT OF DEFENSE OPERATIONS: BACKGROUND, ISSUES, AND OPTIONS FOR CONGRESS 1 (2009), *available at* http://www.fas.org/sgp/crs/misc/R40641.pdf.

[314] *See* Letter from Rep. Bennie G. Thompson, Chairman, CHS, to Michael Hardin, Senior Policy Advisor, US-VISIT, DHS (June 23, 2008), *available at* http://www.regulations.gov/search/Regs/home.html#documentDetail?R=09000064806385ce (expressing concern that DHS's NPRM would shift inherently federal responsibilities to airlines).

[315] The Homeland Security appropriations bill ultimately signed by President Obama in October 2009 mandated $137,000,000 for a pilot program, constituting approximately sixty-one percent of the total funds allocated to USCIS for fiscal year 2010. *See* Department of Homeland Security Appropriations Act, 2010, Pub. L. No. 111-83, tit. IV, 123 Stat. 2142, 2164–67 (2009).

[316] Press Release, DHS, DHS Begins Test of Biometric Exit Procedures at Two U.S. Airports (May 28, 2009), *available at* http://www.dhs.gov/ynews/releases/pr_1243605893203.shtm.

[317] *See, e.g.*, DHS Statement of Regulatory Priorities, 74 Fed. Reg. 64,213, 64,217 (Dec. 7, 2009) (noting that DHS hopes to promulgate a final rule in 2010).

perform its border security and immigration enforcement missions may suffer.[318] The development of a comprehensive entry-exit system, beginning with implementation of US-VISIT exit capability at our nation's airports, is a necessary next step to securing our borders.

F. Proposals

While Congress has shown significant support for enhancing border security in the wake of September 11, enacting comprehensive, common-sense border security legislation has proven challenging. Stakeholders disagree about how best to achieve enhanced border security, as well as how to balance respect for legitimate travel, trade, privacy and civil liberties against security requirements.[319] However, three concepts are integral to border security legislation: (1) requiring DHS to develop and implement a comprehensive border security strategy; (2) mandating a holistic approach that provides appropriate staffing and resources for all of our nation's borders; and (3) developing and implementing reliable, cost-effective technology to serve as a force multiplier.

While all three of these objectives are part of CHS's plan for the 111th Congress,[320] DHS currently lacks a comprehensive plan to achieve border security; instead, it has only piecemeal strategies governing certain individual agencies.[321] This lack of strategy is untenable over the long term. Requiring DHS to develop and implement a comprehensive border security strategy, backed by close congressional oversight, is a first step towards bringing agencies together to work on border security issues. Essential to the development and implementation of such a plan is stakeholder input. Personnel on the front lines of the borders and those who live and work in border communities have much to tell policymakers in Washington about the real-world implications of border security policy.[322] Their input will help ensure that the border security plan has the support of those who will be closest to its implementation.

---

[318] *See* GAO, GAO-10-13, HOMELAND SECURITY: KEY US-VISIT COMPONENTS AT VARYING STAGES OF COMPLETION, BUT INTEGRATED AND RELIABLE SCHEDULE NEEDED 20 (2009).

[319] For an example, see the author's border security principles, *available at* http://homeland.house.gov/SiteDocuments/BorderSecurityPrinciples.pdf, the views of U.S. Chamber of Commerce, *available at* http://www.uschamber.com/issues/index/defense/customstransportation.htm, the views of the ACLU, *available at* http://www.aclu.org/free-speech/aclu-seeks-records-about-laptop-searches-border, and the views of the Border Trade Alliance, *available at* http://homeland.house.gov/SiteDocuments/20090507104137-70024.pdf.

[320] CHS, COMMITTEE ON HOMELAND SECURITY PLATFORM, *available at* http://homeland.house.gov/SiteDocuments/8point.pdf.

[321] *See The Challenge of Aligning Programs, Personnel, and Resources to Achieve Border Security: Hearing Before the H. Comm. on Homeland Sec.*, 110th Cong. 1–2 (2008) (statement of Bennie G. Thompson, Chairman, CHS).

[322] *See generally* Clara Long, *Introduction: Crafting a Productive Debate on Immigration*, 47 HARV. J. ON LEGIS. 167 (2010).

Furthermore, an important element of success is a holistic approach that addresses America's northern, southern, and maritime borders, both at and between the POEs. No longer can we focus exclusively on the needs and challenges of one border at the expense of the others. Personnel, infrastructure, technology, and other resources must be allocated based on legitimate security requirements. DHS must make a full assessment of its existing resources and needs and allocate existing and future resources accordingly. Congress should utilize this assessment to authorize a sufficient number of border security personnel and additional infrastructure as necessary.

We also must develop and deploy reliable, cost-effective technology that allows personnel to do their jobs more efficiently. For example, border security legislation should require DHS to reexamine how to get its troubled "virtual fence" efforts back on track, or what to do as an alternative. It must also mandate that the Department take the steps necessary to implement a government-operated US-VISIT exit solution at airports.

Achieving these legislative goals will not be easy. Border security has become inextricably linked to immigration reform, creating additional political and procedural obstacles to progress.[323] For example, immigration reform supporters oppose freestanding border security legislation, believing that should such enforcement legislation be enacted, there would be little incentive to move forward with immigration reform.[324] In contrast, immigration reform opponents favor an enforcement-only approach. As a result, border policy is currently made only through the annual appropriations process and piecemeal legislation.[325]

---

[323] *See generally* Representative Sheila Jackson Lee, *Why Immigration Reform Requires a Comprehensive Approach That Includes Both Legalization Programs and Provisions to Secure the Border*, 43 HARV. J. ON LEGIS. 267 (2006). Recently, Republican senators have stated that any immigration reform must include improvements to our border security. Indeed, the push for immigration reform has recently jeopardized a parallel push for reforming environmental regulations in the Senate. CNN Wire Staff, *GOP Lawmakers Seek to Halt Immigration Reform Push*, CNN.COM, Apr. 25, 2010, http://www.cnn.com/2010/POLITICS/04/25/immigration.reform/index.html.

[324] *See* Jeffrey Young, *Obama Won't Have Piecemeal Approach*, THE HILL, Mar. 2, 2010, http://thehill.com/homenews/administration/84625-president-obama-wont-have-piecemeal-approach (statement of President Obama); Muzaffar Chishti & Claire Bergeron, *Congress Addresses Immigration But Appears Unlikely to Pass Piecemeal Bills*, MPI, May 15, 2008, http://www.migrationinformation.org/USfocus/display.cfm?id=682; Press Release, League of United Latin Am. Citizens, National Latino Leaders Urge Senate to Oppose Piecemeal Immigration Reform Legislation (Sept. 27, 2006), *available at* http://www.lulac.net/advocacy/press/2006/piecemeal.html (statement of LULAC).

[325] *See* Lee, *supra* note 323, at 273–75 (noting the inadequacy of federal border security policy); *see also* NAT'L COUNCIL OF LA RAZA, FULFILLING THE PROMISE OF IMMIGRATION REFORM, *available at* http://www.nclr.org/files/60371_file_NCLR_Immigration_One_Pager.pdf (noting that "Congressional failure to enact reform has led to piecemeal measures that are introducing chaos into an already broken system"). It is clear that this piecemeal approach to border security has been ineffective and that a more comprehensive approach is needed in order to secure our borders. *The Border Security Challenge: Recent Developments and Legislative Proposals: Hearing Before the H. Comm. on Homeland Sec.*, 110th Cong. 4–5 (2008) (statement of Bennie G. Thompson, Chairman, CHS)("I have long said that the Department

Because of the link between border security and immigration reform, border security legislation will likely be integral to any immigration reform package that could advance through Congress. Recent immigration reform proposals in Congress have incorporated border security provisions that are linked to or would in some way "trigger" immigration benefits.[326] Senate and House authors are currently developing immigration reform legislation to be introduced in the second session of the 111th Congress, and that legislation is likely to include border security measures.[327]

Pursuant to House Rule X, CHS has jurisdiction over the border security functions of DHS, except immigration policy and non-border enforcement.[328] Meanwhile, jurisdiction over immigration policy and interior enforcement resides with the House Judiciary Committee.[329] Because the necessary elements of immigration reform and border security legislation are under the jurisdiction of two committees in the House, jurisdictional challenges may further complicate this already difficult, politically-charged process.

VI. Conclusion: The Path Forward

2011 will mark a decade since the terrorist attacks of September 11. These tragic events prompted Congress and the Executive to make sweeping changes to America's efforts to prevent, prepare for, and respond to disasters and terrorist attacks. However, much more needs to be done, and many obstacles to achieving meaningful security and preparedness remain. It is Congress's responsibility to overcome these obstacles, as our predecessors have done at other critical points in America's history. By following the principles and proposals described above, Congress can move one step closer to fulfilling its solemn oath to the American people.

---

needs a comprehensive strategy for border security. The current piecemeal approach is not the answer").

[326] H.R. 4321, 111th Cong. (2009) (requiring the Secretary of DHS to develop a national border security strategy, increasing the number of personnel at points of entry and providing for comprehensive immigration reform); S. 1639, 110th Cong. (2007) (establishing certain benchmarks to be met before proposed guest worker program can take effect, including improving operational control of the southern border and improving border barriers); S. 2611, 109th Cong. (2006) (requiring the Secretary of DHS to develop a national border security strategy, increasing the number of personnel at points of entry and providing for additional technological infrastructure at points of entry).

[327] *See* Press Release, Sen. Charles E. Schumer (D-N.Y.), Schumer Announces Principles for Comprehensive Immigration Reform Bill in Works in Senate (June 24, 2009), *available at* http://schumer.senate.gov/new_website/record.cfm?id=314990&.

[328] *See* House Rules, *supra* note 25, at 7 R. X.1(i) (establishing the jurisdictional boundaries of CHS).

[329] *See id.* at 7 R. X.1(k)(9) (establishing that the House Judiciary Committee has jurisdiction over immigration and non-border matters).