A Review of the Department of Homeland Security's Missions and Performance

Senator Tom Coburn, M.D.

January 2015

A Review of the Department of Homeland Security's Missions and Performance

A Report by Senator Tom Coburn

Ranking Member

Committee on Homeland Security and Governmental Affairs

U.S. Senate

113th Congress

January 2015

January 3, 2015

Dear Taxpayer,

We Americans are and always have been suspicious—rightfully so—of government infringement on our rights which we hold are inalienable and not derived from the government. Rather, we believe governments are instituted to secure these rights.

Yet, there is and always will be a perpetual struggle between security and liberty in a free society. Liberty requires security, but too much security can result in a loss of liberty. And the erosion of freedoms is rarely restored. We should never have to give up our rights to preserve them, and our Constitution which specifies the rights of the people and the limitations of the government does not even allow for such an exchange.

This balancing act has become increasingly complicated.

The 1995 Oklahoma City bombing and the 9/11/2001 terrorist attacks claimed the lives of thousands, changed the lives of millions, and forever altered how we viewed the world. Every American, no matter what part of the country or the world we live in, could be a possible target of terrorism. But our enemies are not always obvious. They do not wear the uniform of a foreign army. Their weapons are not tanks and bullets. Their tactics are unconventional. Their victims are civilians. And they are among us.

Americans feel uneasy, about both the threats and the responses.

We are willing to endure the inconvenience of arriving at the airport earlier and having our luggage screened, but we are wary of increased government policing and surveillance. We are concerned that despite spending billions of dollars on border security, tens of thousands continue to enter our country illegally and, in 2014, 700 miles of our Southern border were unsecure. The same is true of cyber security. We have spent billions to protect against cyber attacks, yet even White House computers have been susceptible to hacking.

As with so many other government initiatives, Washington is spending billions of dollars hoping that the outcome will equal the expense, but with little evidence that this is indeed the result. This type of reckless spending and failure of leadership have amassed a national debt that poses the most significant threat to our freedom and security as a nation. We are now indebted to some of the very nations that are hostile to the basic values and principles that unite us as a people.

To address the debt threat, Congress must address the other threats to our nation in a fiscally responsible manner. This includes conducting oversight of federal agencies to ensure they are protecting and not infringing upon the rights of the people and also spending taxpayer dollars in the most efficient and effective manner possible.

This report is a comprehensive overview of oversight conducted over the past decade to measure how well DHS is achieving its mission, operating its programs, spending taxpayer funds, complying with the law, and respecting the boundaries established to limit the federal government and protect the rights of law abiding U.S. citizens.

Created after the September 11, 2001 terrorist attacks, DHS is the result of the largest reorganization of government in more than a half century. Today, the Department's spends approximately $61 billion annually and employs more than 240,000 people. It includes many different components, directorates, offices, and programs with a broad range of missions. This report reviews each of DHS's five main missions, where it is falling short with each, and provides recommendations to make the Department more efficient and effective.

The analysis is based upon independent information and evidence as well as oversight conducted by my office and other watchdogs. Where necessary, this report notes where additional oversight is needed to improve transparency and understanding of DHS's programs and performance.

Based upon the available evidence, DHS is not successfully executing any of its five main missions. Many of DHS's programs, in fact, are ineffective and should be reconsidered. One of the most significant challenges DHS faces is Congress. Parochial politics and overlapping

jurisdiction between various congressional committees and subcommittees too often hinder and impede DHS's mission and programs. Reforming DHS, therefore, must begin with changing Congress's approach to homeland security.

The Department must overcome many obstacles, but it confronts each with some great assets, including many of its employees who risk their lives for our security every day. Likewise, Secretary Jeh Johnson has proven to be a capable leader, a transparent partner with Congress, and committed to making tough decisions and improving the Department. I am thankful for his service and leadership, and the dedication of all of the dedicated employees of DHS who work every day to protect our nation, our citizens, and our Constitution. After all, those are the most important duties of our government and those who work for it, including members of Congress.

A new DHS authorization bill has not been passed by Congress since the Homeland Security Act created the department in November 2002. The purpose of this report is to provide an assessment of where the Department is today, and offer recommendations for how it can be improved to strengthen our nation's security while securing the blessings of our liberty.

Sincerely,

Tom A. Coburn, M.D.
Ranking Member
Senate Committee on Homeland Security and
Governmental Affairs

Contents

Executive Summary

The Department of Homeland Security (DHS) is the result of the largest reorganization of government in more than half a century. The reorganization included the consolidation of components and offices from 22 different agencies to create a unified department focusing on homeland security.[1] In 2015, DHS will employ roughly 240,000 people, and spend nearly $61 billion.[2] It is the third largest cabinet agency in government.[3] Since 2003, the Department has spent approximately $544 billion on its programs.[4] Congress has assigned to DHS some of the federal government's most important responsibilities related to securing the nation, including terrorism prevention and protective security, transportation security, border security, immigration enforcement, cybersecurity, and disaster recovery.[5]

This report presents the findings of Senator Tom Coburn's oversight of DHS. Since 2005, Dr. Coburn has been a member of the Senate Homeland Security and Governmental Affairs Committee. He served as the Committee's ranking member during the 113th Congress. The report is based on a review of evidence and information obtained from the department, audits and investigations conducted by watchdogs[6], committee hearings, and open source reporting. Where evidence was lacking, the report suggests opportunities for additional oversight by Congress and other watchdogs.

---

[1] William Painter, "Issues in Homeland Security Policy for the 113th Congress," Congressional Research Service, September 23, 2013.

[2] For information on DHS's annual budget, see: William L. Painter, "Department of Homeland Security: FY2014 Appropriations," Congressional Research Service, April 18, 2014. The estimate for the number of employees at DHS was provided by the Department on its website, see: "About DHS," Department of Homeland Security, at: http://www.dhs.gov/about-dhs, accessed December 31, 2014, December 31, 2014.

[3] "About DHS," Department of Homeland Security, at: http://www.dhs.gov/about-dhs, accessed December 31, 2014.

[4] This figure includes projected spending for FY2014. William Painter, "Total DHS Spending, FY2013-FY2014," Congressional Research Service, Memorandum to the Senate Homeland Security and Governmental Affairs Committee, December 9, 2014.

[5] The Department of Homeland Security receives the largest share of the federal government's spending related to homeland security activities. Other departments, including the Department of Defense, Department of Justice, and Department of Health and Human Services, also receive funding related to homeland security activities. For background, see: Congressional Budget Office, "The Proposed Homeland Security Budget for 2013," September 2012.

[6] Watchdogs include the Department of Homeland Security Office of Inspector General, the Government Accountability Office, and the Congressional Research Service.

Key Findings

Despite spending nearly $61 billion annually[7] and $544 billion since 2003,[8] the Department of Homeland Security is not successfully executing any of its five main missions. Specifically, a review of the Department's performance related to its five main mission areas reached the following key findings:

1. The Department of Homeland Security's primary counterterrorism programs are yielding little value for the nation's counterterrorism efforts.

The Department identifies "preventing terrorism and improving security" as its first mission. But a review of DHS's programs shows that DHS's main domestic counterterrorism programs—including its intelligence initiatives and homeland security grants—are yielding little value for the nation's counterterrorism efforts. Independent reviews—including audits and investigations by watchdogs—show that DHS's intelligence and analysis programs, including its state and local fusion centers and other information sharing programs, are ineffective or providing little value.[9] Similarly, oversight of the more than $38 billion[10] that the Federal Emergency Management Agency (FEMA) has spent on homeland security grants—which were originally intended to improve our ability to prevent terrorist attacks—reveals that DHS has not effectively tracked how these funds are spent and federal dollars often subsidizes routine (and in some cases questionable) expenditures by states, localities, and other groups.[11]

Many of the Department's programs to prevent chemical, biological, radiological, and nuclear attacks have been ineffective and are yielding little value, despite significant expenditures. For example, the National Academies of Sciences identified problems with both

---

[7] For information on DHS's annual budget, see: William L. Painter, "Department of Homeland Security: FY2014 Appropriations," Congressional Research Service, April 18, 2014. The estimate for the number of employees at DHS was provided by the Department on its website, see: Department of Homeland Security, "About DHS," at: http://www.dhs.gov/about-dhs (December 4, 2014).

[8] This figure includes projected spending for FY2014. William Painter, "Total DHS Spending, FY2013-FY2014," Congressional Research Service, Memorandum to the Senate Homeland Security and Governmental Affairs Committee, December 9, 2014.

[9] Permanent Subcommittee on Investigations, "Federal Support for and Involvement in State and Local Fusion Centers: Majority and Minority Staff Report," October 3, 2012; Government Accountability Office, "DHS Intelligence Analysis: Additional Actions Needed to Address Analytic Priorities and Workforce Challenges," GAO 14-397, June 2014; Department of Homeland Security Office of Inspector General, "Homeland Security Information Network Improvements and Challenges," OIG 13-98, June, 2013.

[10] Federal Emergency Management Agency, National Award Summary Report Data as of May 15, 2014.

[11] "Safety at Any Price: Assessing the Impact of Homeland Security Spending in U.S. Cities," A Report by Senator Tom Coburn, Homeland Security and Governmental Affairs Committee, December 2012.

of the systems that DHS purchased to detect biological[12] or radiological[13] attacks, and DHS ultimately halted the deployment of new technologies after more than five billion was spent on the respective projects.[14]

The Department has also struggled to execute its responsibilities to provide or improve the nation's physical security, including its work with the private sector to support critical infrastructure security.[15] For example, DHS has spent more than a half a billion dollars over the past seven years on its program to create standards for and regulate the security of chemical facilities at risk of potential terrorist attacks.[16] But the program has experienced significant problems, and 99 percent of all the chemical facilities that were supposed to be overseen by the program had not been inspected as of June 2014.[17] Oversight also reveals problems with DHS's initiatives to share information with critical infrastructure owners and operators.[18]

DHS has also struggled with its protective security responsibilities. Multiple audits have identified problems in the Federal Protective Service's (FPS) management of its responsibilities for securing federal buildings.[19] Even the U.S. Secret Service (USSS) has recently experienced challenges executing its responsibilities for securing the White House and the President.[20]

---

[12] Institute of Medicine and the National Research Council of the National Academies, "BioWatch and Public Health Surveillance: Evaluating Systems for the Early Detection of Biological Threats: Abbreviated Version," 2011.
[13] National Research Council of the National Academies, "Evaluating Testing Costs, and Benefits of Advanced Spectroscopic Portals: Final Report," 2011, p. 2.
[14] See the discussion below about BioWatch and Domestic Nuclear Detection Office's radiation monitors.
[15] Government Accountability Office, "Critical Infrastructure Protection: DHS Action Needed to Enhance Integration and Coordination of Vulnerability Assessment Efforts," GAO-14-507, September 15, 2014.
[16] Senator Tom Coburn, "Chemical Insecurity: An Assessment of Efforts to Secure the Nation's Chemical Facilities from Terrorist Threats," U.S. Senate Homeland Security and Governmental Affairs Committee, July 2014.
[17] Ibid.
[18] Ibid, p.3.
[19] Government Accountability Office, "Challenges Associated with Federal Protective Services' Contract Guards and Risk Assessments at Federal Facilities," GAO-14-128T, October 30, 2013; Department of Homeland Security Office of Inspector General, "Effects of a Security Lapse on FPS' Michigan Guards Services Contract," OIG-12-100 (Revised), August 2012, p.6.
[20] "Executive Summary of the U.S. Department of Homeland Security Report on the White House Incursion Incident of September 19, 2014," Department of Homeland Security, November 13, 2014; Joseph Hagin, Thomas Perrelli, Danielle Gray, Mark Filip, United States Secret Service Protective Mission Panel, "Executive Summary to Report from the United States Secret Service Protective Mission Panel to the Secretary of Homeland Security," December 15, 2014.

2. The nation's borders remain unsecure.

The Department's second mission is to secure and manage the nation's borders. While DHS officials have claimed that the border is more secure than ever, evidence reviewed shows that vast spans of the Southern and Northern borders remain uncontrolled and are vulnerable to illegal entry. In 2014, 700 hundreds of miles of the Southern border were not secure, since DHS and its component, Customs and Border Protection (CBP), had not deployed assets to control these areas.[21] DHS has little control at the Northern border with Canada with very few resources deployed and thousands of miles uncontrolled.[22]

Several factors contribute to DHS's inability to secure the borders. Until recently, DHS did not have a comprehensive strategy for securing the border. Another factor is DHS's inability to effectively use its assets, such as its aerial surveillance equipment, to monitor the borders and assist personnel on the ground.[23] The Department also faces a potentially significant problem of corruption in its workforce assigned to secure the border.[24] Vulnerabilities in Southern and Northern border security suggest that adversaries committed to gaining illegal entry into the United States—including drug trafficking organizations and other adversaries—have a reasonable chance of defeating DHS's border security defenses, creating a potential threat to national security and public safety. The uncontrolled border also invites more illegal immigration, which will continue to be a problem until both our borders are more secure and our nation's immigration laws are being enforced.

The Department has faced challenges with its other responsibilities related to border security, including safeguarding trade and travel into the United States. For example, despite spending nearly $5 billion on port security projects[25], DHS has struggled to execute its

[21]Committee minority staff review and analysis of documents provided by DHS and Customs and Border Protection and DHS.

[22] Committee minority staff review and analysis of documents provided by DHS and Customs and Border Protection and DHS; Government Accountability Office, Border Security: Enhanced DHS Oversight and Assessment of Interagency Coordination is Needed for the Northern Border, GAO-11-97, December 17, 2010. Government Accountability Office, "Border Security: Opportunities Exist to Ensure More Effective Use of DHS's Air and Marine Assets," GAO-12-518, March 2012, Highlights.

[23] DHS Office of Inspector General, CBP's Use of Unmanned Aircraft Systems in the Nation's Border Security, OIG-12-85, May 2012,.

[24]Government Accountability Office, "Border Security: Additional Actions Needed to Strengthen CBP Efforts to Mitigate Risk of Employee Corruption and Misconduct," GAO-13-59, December 4, 2012, Highlights.

[25] The Department has several programs for port security. According to information provided to the minority staff by DHS, the Department has spent approximately $5.167 billion on its various initiatives related to port security since 2002, including $2.958 billion on the Port Security Grant Program, 959 million on the Container Security Initiative, 411.9 million on the Customs-Trade Partnership Against Terrorism, 336.7 million on the Automated

responsibilities for securing U.S. ports[26], one of the nation's most important critical infrastructure assets. DHS spending on programs to secure port facilities, infrastructure, and cargo have not accomplished their objectives.[27] While DHS has made progress in its work to secure aviation systems, a review of our aviation security programs, and the oversight work that has been done on the Transportation Security Administration (TSA), reveal key areas where DHS has struggled, as well as opportunities for DHS and TSA to improve strategy and programs for safeguarding air travel.[28]

3. The Department of Homeland Security is not effectively administering or enforcing the nation's immigration laws, and some of the immigration programs the agency manages have significant vulnerabilities.

The third mission of DHS's is to administer and enforce our nation's immigration laws. Evidence shows DHS is not successfully accomplishing either responsibility. The Department has struggled with administering the nation's immigration system, including vetting, processing, and tracking immigration benefits for non-citizens.[29] Nor has DHS effectively tracked and monitored the population of people who have overstayed their visas. DHS's struggle to administer the immigration system raises questions about its ability to effectively manage any large program to provide new immigration benefits to people currently living in the United States illegally, as was ordered by President Obama on November 20, 2014.[30]

The Department consistently has not enforced the nation's immigration laws. Immigration experts, including some former DHS officials, point out that a person living in the United States illegally faces an extremely slim chance of facing consequences for violating

---

Targeting System, 60 million on the Secure Freight Initiative, $21.8 million on the Coast Guard's waterways and coastal security efforts, and $420 million on the Transportation Worker's Identification Credential. Committee staff analysis December 2014.

[26] "Evaluating Port Security: Progress Made and Challenges Ahead," Senate Homeland Security and Governmental Affairs Committee hearing, June 4, 2014.

[27] See the review of port security initiatives in the section of the report on DHS's second mission.

[28] See the discussion on the Transportation Security Administration's aviation security initiatives.

[29] DHS Office of Inspector General, "U.S. Citizenship and Immigration Services' Progress in Transformation," OIG-12-12, November 2011; Aliya Sternstein, "After Delays, USCIS Sets New Deadline for Digital Immigration Records," NextGov.com, July 29, 2014; William A. Kandel, "U.S. Citizenship and Immigration Services' Immigration Fees and Adjudication Costs: Proposed Adjustments and Historical Context," Congressional Research Service, RL34040, July 16, 2010

[30] Executive Actions on Immigration, U.S. Citizenship and Immigration Services, at: http://www.uscis.gov/immigrationaction, December 31, 2014.

federal immigration laws.[31] Although DHS instituted a policy to focus its law enforcement and removal efforts on criminal aliens, the Department has even failed to ensure that criminal aliens are detained or removed from the country, putting public safety at risk.[32] The recent announcement to end the Secure Communities program and replace it with a new initiative suggests a further shift away from immigration enforcement, including enforcement related to criminal aliens.[33] The Department's lax approach to immigration law enforcement, and broad applications of prosecutorial discretion with regard to enforcing immigration laws also exacerbates DHS's challenge securing the border. Rather than deterring illegal immigration, lax immigration enforcement creates an expectation that people entering the nation illegally or violating the terms of their visa will be allowed to stay, facing no consequences.

The Department of Homeland Security also oversees two immigration benefit programs with significant vulnerabilities, presenting a threat to national security and public safety. Specifically, Immigration and Customs Enforcement (ICE) oversees the Student and Exchange Visitor Program (SEVP), which is currently used by more than one million people to gain entry into the United States. DHS is not effectively managing this program by ensuring its participants follow the rules, creating significant vulnerabilities to national security and public safety.[34] In the past, people plotting terrorist attacks, including several of the 9/11 hijackers, were in the United States using student visas.[35]

DHS, through its component U.S. Citizenship and Immigration Services (USCIS), manages another immigration benefit program, the Employment-Based Fifth Preference (EB-5) visa program, which allows immigrants to gain entry into the United States if they make a business investment totaling $500,000 or $1,000,000. Several reviews of this program, including

[31] Brian Bennett, "High deportation figures are misleading," Los Angeles Times, April 1, 2014. According an analysis by experts writing for the Council on Foreign Relations in 2013, the chance of an illegal immigrant being removed by DHS is approximately 3.26 percent. Council on Foreign Relations, "Managing Illegal Immigration to the United States: How Effective Is Enforcement?," May 2013, p. 29.

[32] "ICE's Release of Immigration Detainees," Department of Homeland Security Office of Inspector General, OIG-14-116, August 2014.

[33] Secretary Jeh Johnson, Memorandum for Thomas S. Winkowski, Megan Mack, Phil McNamara, "Subject: Secure Communities," November 20, 2014. Secretary Johnson wrote: 'The Secure Communities program, as we know it, will be discontinued."

[34] Government Accountability Office, "Student and Exchange Visitor Program: DHS Needs to Assess Risk and Strengthen Oversight of Foreign Students with Employment Authorization," March 7, 2014.

[35] An ICE official told Committee staff that approximately 36 convicted terrorists came to the country using various forms of student visas. Minority committee staff interview with ICE HSI Special Agent Brian Smeltzer, Unit Chief, Counterterrorism and Criminal Exploitation Unit, July 1, 2014.

an independent audit[36] and internal reviews apparently ordered by the White House[37] and DHS Secretary[38], identified significant vulnerabilities in this EB-5 visa program, including the potential for it to be exploited by criminals, terrorists, foreign government agencies and intelligence operatives, and other adversaries. Oversight of the program, including surveying 430 regional centers, raised additional questions about the EB-5 visa program and why the Department continues to operate and expand a program known to be vulnerable to criminal and national security threats.[39]

4. The Department of Homeland Security is struggling to execute its responsibilities for cybersecurity, and its strategy and programs are unlikely to protect us from the adversaries that pose the greatest cybersecurity threat.

The Department's fourth mission is to "safeguard and secure cyberspace." Attacks against government and private networks have become a significant threat to the nation and our economy. DHS spends more than $700 million annually[40] on a range of cybersecurity programs, including its efforts to assist the Office of Management and Budget (OMB) with federal agency information security, as well as various initiatives to help the private sector and critical infrastructure owners and operators with their cybersecurity. Other entities within DHS, including the Secret Service and ICE, have investigative responsibilities for cybersecurity.

Repeated audits by the Inspector General have found that the Department's own offices and employees do not always comply with federal rules and policies for agency cybersecurity. [41] It is also unclear whether DHS's programs for assisting the private sector in preventing,

---

[36] DHS Office of Inspector General, "United States Citizenship and Immigration Services' Employment-Based Fifth Preference (EB-5) Regional Center Program," OIG-14-19, December 2013.
[37] Forensic Assessment of Financial Flows Related to EB-5 Regional Center, Document Marked Draft and Pre-Decisional, National Security Staff.
[38] Undated Memorandum, U.S. Customs and Immigration Enforcement on Implications of U.S. Immigration and Customs Case Against Procurement Agent. U.S. Immigration and Customs Enforcement, Homeland Security Investigations, "EB-5 Program Questions from DHS Secretary." Senator Grassley published a redacted copy of the document on his website, at: http://www.grassley.senate.gov/sites/default/files/issues/upload/EB-5-12-12-13-ICE-memo-security-vulnerabilities.pdf, accessed: December 28, 2014.
[39] See the below discussion of Senator Coburn's effort to survey 430 regional centers.
[40] Id. As of FY2013, NPPD had 348 FTEs in these programs.
[41] Office of Inspector General, "Evaluation of DHS' Information Security Program for Fiscal Year 2013," Department of Homeland Security, OIG-14-09, November 2013; Office of Inspector General, "Evaluation of DHS' Information Security Program for Fiscal Year 2014," Department of Homeland Security, OIG-15-16, December 12, 2014.

mitigating, or recovering from cybersecurity incidents are providing significant value or are worth the tax dollars spent on them.

Although the Department's law enforcement agencies are involved in arresting criminals who violate our laws and attack our nation's information systems, a majority of the Department's resources for cybersecurity are spent on a strategy to help the government and the private sector defend its networks. The nature of cybersecurity threats—and the ability of adversaries to continuously develop new tools to defeat network defenses—means that DHS's strategy for cybersecurity, which focuses primarily on vulnerability mitigation, will not protect the nation from the most sophisticated attacks and cybersecurity threats.

5. The Department of Homeland Security is federalizing the response to manmade and natural disasters by subsidizing state, local, and private sector activity.

The Department spends the largest share of its budget—$14 billion or approximately twenty-three percent of DHS's total departmental enacted budget of $61 billion for FY2014[42] — on the Federal Emergency Management Agency (FEMA). This component is dedicated to the Department's fifth mission: strengthening national preparedness and resilience. This $14 billion is devoted to a range of spending programs that are aimed to help the nation both prepare for and respond to natural disasters and other emergencies, including preparedness grants, disaster relief services and assistance, and the National Flood Insurance Program.

Oversight of FEMA's programs shows increasing expenditures with little evidence of value, raising serious questions about the extent to which FEMA's initiatives are making our nation better prepared for or more resilient to natural disasters. For example, since 2002, DHS has spent $170 billion on FEMA and its programs, of which $37.6 billion was related to Hurricane Katrina.[43] Much of this spending is focused on subsidizing state, local, and private sector spending on emergency management; public safety; clean-up and rebuilding efforts through homeland security grants: after-the-fact disaster relief for events that occurred weeks, months, and years ago; and subsidized property insurance for people who live in flood zones.

---

[42] Department of Homeland Security, Congressional Budget Justification FY 2015, Volume I, FY2014 Enacted Column, pg. 10 and 13, includes funding for the Disaster Relief Fund and the National Flood Insurance Program, available at http://www.dhs.gov/sites/default/files/publications/DHS-Congressional-Budget-Justification-FY2015.pdf .

[43] See a detailed discussion of FEMA's programs in the section of the report reviewing the Department's fifth mission.

Structural problems in FEMA's programs result in federal funding being spent inefficiently, disaster assistance being provided to state and localities for many events that would not have been declared disasters twenty years ago[44], and a flood insurance program that encourages citizens to build and rebuild homes and businesses in flood plains, where they are more vulnerable to disaster.

Few Americans would disagree that there is a role for the federal government to step in and provide aid to state and local authorities in order to help save lives and repair our communities after a natural disaster or terrorist attack. The nation is thankful that an organization like FEMA is on call to provide help when serious disasters strike. To its credit, FEMA has improved its ability to quickly mobilize and provide assistance since Hurricane Katrina. It is precisely because of the critical role that FEMA plays in our darkest hours that Congress must take a critical eye to its current challenges.

Recommendations

The report makes the following recommendations for principles for reforming DHS and the nation's approach to homeland security.

The most important recommendation is for Congress itself—reforming Congress's dysfunctional approach to overseeing the Department and setting its priorities, including overcoming the political and parochial interests that too often shape our programs, even those that relate to our national security.

Congress and the Department must refocus its programs and missions on national priorities and the federal government's duties related to domestic security, where DHS has lead responsibility. Specifically, the following recommendations are made for the Department's five main mission areas:

- DHS should refocus its counterterrorism and protective security mission on areas where it has a lead responsibility within the federal government and can make measurable improvements in the nation's security, such as securing the nation's borders, skies, and waterways, effectively tracking and monitoring persons entering and exiting the

[44] "An Imperfect Storm: How Outdated Federal Rules Distort the Disaster Declaration Process and Fleece Taxpayers," Senator Tom Coburn, U.S. Senate Homeland Security and Governmental Affairs Committee, December 31, 2014.

country, and enforcing immigration laws. DHS must successfully execute its federal protective security responsibilities.

- The Department must prioritize securing the border. This includes improving DHS's use of existing resources, as well as increasing transparency to Congress and the public about the state of border security and what resources are needed.
- DHS must improve its administration of the immigration system and recommit to enforcing the rule of law to deter illegal immigration. DHS should reform or end immigration benefit programs that are vulnerable to criminal and national security threats.
- For cybersecurity, DHS's first job should be to set an example by becoming a model of effective cybersecurity and assisting OMB with its oversight of civilian agency information security. For its other cybersecurity programs, DHS should reconsider its current strategy, which focuses largely on vulnerability mitigation and which will likely prove ineffective in preventing the most serious cyber security threats.
- For disaster relief and emergency management, federal aid should be focused on emergencies and disasters that require the federal government to step in to help American citizens whose lives are in jeopardy, and which truly overwhelm the ability of state and local governments. FEMA's programs for subsidizing state and local emergency management and public safety, including the preparedness grant programs and disaster assistance for routine events, should be ended.

While reconsidering how the Department can achieve its missions and execute its responsibilities that are national priorities and clear responsibilities of DHS and the federal government, Congress should end DHS's many programs that are unnecessary, ineffective, or duplicative of other efforts.

Another important recommendation is that Congress must give the Secretary of Homeland Security the authority to lead, manage, and reform the Department and change its dysfunctional culture. For too long, the Department's leadership has been unable to effectively manage its many components and directorates, and unify the Department to achieve its missions and responsibilities. Secretary Jeh Johnson has made an admirable attempt to manage the Department, including his "Unity of Effort" initiative, but much work remains to implement effective management and unity across the Department. Congress should entrust DHS's

leadership with real authority to manage the Department and change its culture. This will include reforming its workforce.

Congress and DHS must also focus on earning and restoring the American people's trust. This includes ensuring that all of the Department's programs and operations are consistent with the American people's Constitutional rights and the proper role of the federal government. Too many of DHS's programs have faced questions in this regard. We have also witnessed incidents where the Department's programs have raised concerns about excessive federal authority or otherwise contributed to some of the public's distrust of law enforcement. Congress has a duty to conduct vigorous and persistent oversight of DHS's programs to ensure that they are operating in a manner consistent with the Constitution.

* * *

In his farewell address to the Senate, Dr. Coburn stated: "To know how to reach a destination, you must first know where you are. And without oversight—effective, vigorous oversight—you will never solve anything."[45] A decade of oversight of DHS shows there is much work to be done before the Department of Homeland Security reaches the destination intended for it by Congress and the American people.

[45] Senator Tom Coburn, Remarks on the Senate Floor, December 11, 2014.

Part I: Reviewing the Department of Homeland Security's Five Top Missions and Other Main Program Areas

Assessing the Department of Homeland Security's performance twelve years after its creation starts with considering some basic questions. Is DHS succeeding in accomplishing the missions that Congress and the administration have directed it to execute? Are the components responsible for accomplishing these missions succeeding in accomplishing their objectives? Answering these questions will help Congress understand whether the Department is succeeding or whether its programs and initiatives should be reformed to allow it to succeed.

Part I of this report reviews whether DHS is effectively accomplishing the five missions the Department identified for itself in its current strategic plan, which was created in 2012 and set to guide the Department's strategy for FY 2012 through FY 2016.[46] These five key missions are the same as those identified by Secretary Jeh Johnson in public statements, including at his confirmation hearing before the Senate Homeland Security and Governmental Affairs Committee in 2013.[47]

This review is an analysis of evidence about DHS's performance executing these missions, including audits by watchdog groups such as the Government Accountability Office (GAO) and the Office of Inspector General (OIG), the oversight work by Congress, and judgments about whether the evidence indicates that the mission is being accomplished.

[46] "Department of Homeland Security Strategic Plan: Fiscal Years 2012-2016," Department of Homeland Security, February 2012, http://www.dhs.gov/xlibrary/assets/dhs-strategic-plan-fy-2012-2016.pdf, accessed December 4, 2014.
[47] "Statement of Jeh Charles Johnson on His Nomination to Serve as Secretary of the U.S. Department of Homeland Security," Senate Homeland Security and Governmental Affairs Committee, November 13, 2013.

Mission 1—Preventing Terrorism and Improving Security

Overview

When he signed the Homeland Security Act of 2002, President George W. Bush cited the threat of terrorism as the main reason for creation of the Department of Homeland Security.[48] The Department's current strategic plan lists "preventing terrorism and improving security" as its top mission.[49] In a February 2014 speech, Secretary Jeh Johnson stated, "Preventing terrorist attacks on the homeland is and should remain the cornerstone of homeland security."[50]

But a review of DHS's programs, including those related to counterterrorism, raise questions about whether counterterrorism is actually DHS's primary mission, and also whether these programs are succeeding in making the United Sates safe from the threat of a terrorist attack on American soil. Several of the Department's key initiatives that are described as counterterrorism programs, including its intelligence programs and homeland security grants, appear to do little to improve the nation's ability to prevent terrorist attacks.[51] Moreover, whether the Department's programs to prevent specific types of terrorist attacks, including chemical, biological, radiological, nuclear and explosives (CBRNE), are effective or yielding measurable improvements in security remains an open question.[52]

---

[48] President George W. Bush, "Statement on Signing the Homeland Security Act of 2002," November 25, 2002, at: http://www.presidency.ucsb.edu/ws/index.php?pid=64224, accessed August 1, 2014. President Bush stated: "The Act restructures and strengthens the executive branch of the Federal Government to better meet the threat to our homeland posed by terrorism. In establishing a new Department of Homeland Security, the Act for the first time creates a Federal department whose primary mission will be to help prevent, protect against, and respond to acts of terrorism on our soil."

[49] "Department of Homeland Security Strategic Plan: Fiscal Years 2012-2016," Department of Homeland Security, February 2012.

[50] Sec. Jeh Johnson, "Remarks at the Woodrow Wilson Center," February 7, 2014, at: http://www.dhs.gov/news/2014/02/07/remarks-secretary-homeland-security-jeh-johnson-woodrow-wilson-center.

[51] Permanent Subcommittee on Investigations, "Federal Support for and Involvement in State and Local Fusion Centers: Majority and Minority Staff Report," October 3, 2012; Government Accountability Office, "DHS Intelligence Analysis: Additional Actions Needed to Address Analytic Priorities and Workforce Challenges," GAO 14-397, June 2014; "Safety at Any Price: Assessing the Impact of Homeland Security Spending in U.S. Cities," A Report by Senator Tom Coburn, Homeland Security and Governmental Affairs Committee, December 2012; Government Accountability Office, "Managing Preparedness Grants and Assessing National Capabilities: Continuing Challenges Impede FEMA's Progress," GAO-12-526T, March 20, 2012, highlights page.

[52] The history of DHS's programs to detect and prevent CBRNE attacks is presented below. See for example: GAO analyzed the decision to cancel BioWatch Generation 3 project and found that the decision to cancel the project "raises potential challenges" for the currently deployed Gen-2 system," given questions about the technology's effectiveness and the need to replace some of the Gen-2 systems equipment moving forward. Government Accountability Office, "Observations on the Cancelation of BioWatch Gen-3 and Future Considerations of the Program," GAO-14-267T, June 10, 2014; Government Accountability Office, "Combating Nuclear Smuggling:

Examining the evidence and oversight work done concerning the Department's missions to provide or improve physical security—including supporting private sector critical infrastructure protection—raises serious questions about how effective these initiatives have been. For example, over the past eight years, taxpayers have spent more than half a billion dollars on DHS's Chemical Facilities Anti-Terrorism Standards (CFATS) program, yet the Department has not set up an effective chemical security regulatory program or measurably reduced the risk of an attack on our chemical infrastructure.[53] Similarly, audits and troubling incidents reveal that the Department's Federal Protective Service is struggling with the mission of protecting federal buildings[54], while new questions are being asked about the U.S. Secret Service's performance protecting the White House and President of the United States.[55]

Twelve years after its creation, Congress and the Department need to review DHS's performance in these areas and determine whether "preventing terrorism and enhancing security" remains DHS's first mission, and reconsider what the appropriate role is for the Department in the federal government's counterterrorism strategy and programs. If DHS's programs for counterterrorism are not yielding measurable results and improving our nation's ability to prevent terrorism, or if they are duplicative of other federal initiatives, DHS's resources should be saved or refocused on areas where the Department has a primary responsibility and can make a measurable improvement to the nation's security.

Reviewing DHS's Programs and Responsibilities Related to Preventing Terrorism

On April 15, 2013, the nation experienced a major terrorist attack when two improvised explosive devices detonated at the Boston marathon, killing three people and wounding

---

Lessons Learned from Canceled Radiation Portal Monitor Program Could Help Future Acquisitions," GAO-13-256, May 2013.

[53] Senator Tom Coburn, "Chemical Insecurity: An Assessment of Efforts to Secure the Nation's Chemical Facilities from Terrorist Threats," U.S. Senate Homeland Security and Governmental Affairs Committee, July 2014.

[54] Government Accountability Office, "Challenges Associated with Federal Protective Services' Contract Guards and Risk Assessments at Federal Facilities," GAO-14-128T, October 30, 2013; Department of Homeland Security Office of Inspector General, "Effects of a Security Lapse on FPS' Michigan Guards Services Contract," OIG-12-100 (Revised), August 2012, p.6.

[55] "Executive Summary of the U.S. Department of Homeland Security Report on the White House Incursion Incident of September 19, 2014," Department of Homeland Security, November 13, 2014; Joseph Hagin, Thomas Perrelli, Danielle Gray, Mark Filip, United States Secret Service Protective Mission Panel, "Executive Summary to Report from the United States Secret Service Protective Mission Panel to the Secretary of Homeland Security," December 15, 2014.

hundreds.[56] In the aftermath of that atrocity, federal, state, and local law enforcement began investigating the incident and hunting the terrorists who committed the act. After Dzhokar Tsarnaev was captured, Congress and the administration moved to the secondary, but important, task of questioning why the event happened, and what could have been done to prevent it. This included an interagency review conducted by the Inspectors General of the Intelligence Community, Congressional hearings, and after action reviews. These reviews provide a window into the question of what role DHS, in relation to the Intelligence Community, can or should play in preventing terrorist attacks.

On April 10, 2014, the Department released a 19-page report, "*Boston Marathon Bombing: The Positive Effect of Planning and Preparation on Response*," which was reportedly written in response to an after-action review ordered by Sec. Janet Napolitano.[57] The report largely focused on the constructive role that pre-event training and planning had in facilitating the swift and effective response. It also highlights constructive roles that DHS and entities it supports provided after the bombing, including assisting other federal and state law enforcement and intelligence activities.[58] However, the DHS review does not identify actions that the Department or its components should have taken to prevent the Boston Marathon bombing attack and provides few "lessons learned" or recommendations for how DHS can play a constructive role in preventing future terrorist attacks.[59] Nor did it mention the Department's Office for Bombing Prevention.

---

[56] "Unclassified Summary of Information Handling and Sharing Prior to the April 15, 2013 Boston Marathon Bombing," Prepared by the Inspectors General of the Intelligence Community, Central Intelligence Agency, Department of Justice, and Department of Homeland Security, April 10, 2014, at: http://www.dni.gov/files/documents/ICIG_Forum_Boston_Marathon_Bombings_Review_-_Unclassifed_Summary.pdf , accessed August 4, 2014.

[57] Federal Emergency Management Agency, "Boston Marathon Bombings: The Positive Effect of Planning and Preparation on Response," Department of Homeland Security, Lessons Learned Information Sharing, https://www.llis.dhs.gov/sites/default/files/Boston%20Marathon%20Bombings%20Positive%20Effects%20of%20Planning.pdf, accessed December 29, 2014.

[58] Ibid.

[59] The report includes a few recommendations for future activities DHS could take to prevent future terrorist attacks and specifically for "Countering IED Threats," including "expand and promote activities such as suspicious activity reporting and private sector security measures" and "researching next generation technology to stay ahead of advances in wireless technology." But the topline finding of the report, identified in reports' two sentence summary, was: "Response plans and pre-established coordination centers enabled first responders and emergency managers to coordinate this extraordinary response effort and save lives." Federal Emergency Management Agency, "Boston Marathon Bombings: The Positive Effect of Planning and Preparation on Response," Department of Homeland Security, Lessons Learned Information Sharing. Federal Emergency Management Agency, "Boston Marathon Bombings: The Positive Effect of Planning and Preparation on Response," Department of Homeland Security, Lessons Learned Information Sharing.

Though there are open questions about the extent to which DHS's grant funding to Massachusetts and Boston was useful before and after the attack[60], evidence suggests that DHS's support for training activities, in particular, played a constructive role in preparing state and local first responders for the emergency and swift response.[61] But the absence of an in-depth discussion in the "Lessons Learned" report about what additional roles DHS could play in preventing future terrorist attacks raises questions about whether counterterrorism—and specifically, terrorism prevention—truly is the Department's first mission, and whether that mission has transformed into preparing to recover from terrorist attacks.[62]

The Intelligence Community Inspectors General report on information handling and sharing prior to the Boston Marathon bombings raised additional questions about what role DHS can or should play in stopping domestic terrorist attacks.[63] The report looked at three DHS components' potential role in preventing terrorism: U.S. Citizenship and Immigration Services ("overseeing and adjudicating immigration benefits"); U.S. Customs and Border Protection ("vets people and goods entering and exiting the United States"); and TSA ("which secures U.S. transportation systems").[64] According to the Inspectors General, the biggest role that DHS could have played to help prevent this terrorist attack in the United States since September 11, 2001 would have been to more accurately report and screen Tamerlan Tsarnaev's outbound and inbound travel to and from Russia in 2012, which the FBI potentially could have used to reopen

[60] For example, see the Senate Homeland Security and Governmental Affairs Committee's July 10, 2013 hearing on the Boston Marathon Bombings. The usefulness of DHS's grant funding for Massachusetts and Boston was also discussed at the Committee's September 9, 2014 hearing on state and local law enforcement oversight. A DHS official asserted that an infrared camera was instrumental in locating Dzhokhar Tsarnaev when he was lying injured in a boat; however, Senator Coburn inserted for the record a October 16, 2013 Boston Globe article that reports that the owner of the boat is responsible for spotting Tsarnaev as he called 911 after inspecting the boat and seeing blood splattered. (See: David Abel, "Boat owner seeks to clarify record on Tsarnaev capture," The Boston Globe, October 16, 2013.)

[61] Federal Emergency Management Agency, "Boston Marathon Bombings: The Positive Effect of Planning and Preparation on Response," Department of Homeland Security, Lessons Learned Information Sharing, https://www.llis.dhs.gov/sites/default/files/Boston%20Marathon%20Bombings%20Positive%20Effects%20of%20Planning.pdf, accessed December 29, 2014.

[62] Ibid.

[63] "Unclassified Summary of Information Handling and Sharing Prior to the April 15, 2013 Boston Marathon Bombing," Prepared by the Inspectors General of the Intelligence Community, Central Intelligence Agency, Department of Justice, and Department of Homeland Security, April 10, 2014, at: http://www.dni.gov/files/documents/ICIG_Forum_Boston_Marathon_Bombings_Review_-_Unclassifed_Summary.pdf , accessed August 4, 2014.

[64] Ibid, p.6.

its previously closed investigation of Tsarnaev[65] and to improve database management procedures.[66] Like DHS's own after-action report, the Intelligence Community Inspectors General report did not examine or offer recommendations about how DHS's grant funding or intelligence and information sharing programs could have played a role in preventing the bombing.[67]

DHS's Intelligence and Information Sharing Programs Provide Little Value

Intelligence analysis and information sharing was one of the ways that Congress intended DHS to prevent terrorist attacks. Specifically, the Homeland Security Act of 2002 authorized DHS's original intelligence mission, which was to "receive, analyze, and integrate law enforcement and intelligence information" to identify, assess, and detect terrorist threats against the United States, and understand these threats "in light of actual and potential vulnerabilities to the homeland."[68] The law also directed DHS to improve information sharing within the federal government and with state, local, and private sector partners "to assist in the deterrence, prevention, preemption of, or response to, terrorist attacks against the United States."[69]

Since 2002, the Department has pursued this intelligence mission through several initiatives led by the Office of Intelligence and Analysis, including its support of the state and local fusion center program, the creation of its own public-private information sharing environment (the Homeland Security Information Network or "HSIN"), and through its analysts' production of intelligence products for national, state and private sector consumers.[70] DHS also maintains separate intelligence programs within seven of its components.[71] After

[65] For more information, see: "Lessons Learned from the Boston Marathon Bombing: Improving Intelligence and Information Hearing," Senate Homeland Security and Governmental Affairs Committee Hearing, April 30, 2014.
[66] The Inspectors General's only recommendation related to DHS was: "The DOJ and DHS OIGs recommend that the FBI and DHS clarify the circumstances under which JTTF personnel may change the display status of a TECS record, particularly in closed cases." "Unclassified Summary of Information Handling and Sharing Prior to the April 15, 2013 Boston Marathon Bombing," Prepared by the Inspectors General of the Intelligence Community, Central Intelligence Agency, Department of Justice, and Department of Homeland Security, April 10, 2014, at: http://www.dni.gov/files/documents/ICIG_Forum_Boston_Marathon_Bombings_Review_-_Unclassifed_Summary.pdf , accessed August 4, 2014, p. 25.
[67] Ibid.
[68] P.L. 107-296, Nov. 25, 2002, §101b(1), 116 STAT. 2147.
[69] P.L. 107-296, Nov. 25, 2002, §101b(1), 116 STAT. 2146.
[70] "More About the Office of Intelligence and Analysis Mission," Office of Intelligence and Analysis, Department of Homeland Security, at: http://www.dhs.gov/more-about-office-intelligence-and-analysis-mission#3, accessed December 31, 2014.
[71] Ibid. See information about the DHS intelligence enterprise.

twelve years, evidence suggests that the core initiatives of the DHS Office of Intelligence and Analysis (I&A) are yielding very little value for the nation's counterterrorism mission, and do not provide much useful intelligence or meaningful information sharing at the state and local level.[72]

One of the ways that DHS intended to support the nation's counterterrorism mission through enhanced intelligence information sharing was by supporting state and local fusion centers, which are meant to serve as venues and hubs of intelligence sharing between federal, state, and local officials. The Department spent between $289 million and $1.4 billion supporting the approximately 70 fusion centers across the nation between 2003 and 2011.[73] In 2012, the Permanent Subcommittee on Investigation (PSI) completed a two-year bipartisan investigation of DHS's support for the state and local fusion center program, which found that DHS's work with the fusion centers had not produced useful intelligence to support federal counterterrorism efforts.[74] The PSI investigation revealed that fusion centers "often produced irrelevant, useless or inappropriate intelligence reporting to DHS, and many produced no intelligence reporting whatsoever."[75] A November 2014 GAO audit found that the Department remains unable either to measure the fusion centers' performance in contributing to homeland security or to accurately track and account for the millions of dollars in federal grant funding they receive.[76]

Besides fusion centers, another way that DHS was supposed to improve the nation's intelligence and information sharing capabilities was through the Homeland Security Information Network (HSIN), a computer system that was created to allow DHS to share sensitive but unclassified information with federal, state, and local partners.[77] A 2013 audit by the Department's Inspector General found that after nine years developing the information

---

[72] Permanent Subcommittee on Investigations, "Federal Support for and Involvement in State and Local Fusion Centers: Majority and Minority Staff Report," October 3, 2012; Government Accountability Office, "DHS Intelligence Analysis: Additional Actions Needed to Address Analytic Priorities and Workforce Challenges," GAO 14-397, June 2014

[73] Permanent Subcommittee on Investigations, "Federal Support for and Involvement in State and Local Fusion Centers: Majority and Minority Staff Report," October 3, 2012, p.3.

[74] Ibid, p.1.

[75] Ibid., p. 2.

[76] Government Accountability Office, "Information Sharing: DHS Is Assessing Fusion Center Capabilities and Results, but Needs to More Accurately Account for Federal Funding Provided to Centers," GAO-15-155, November 4, 2014.

[77] "Homeland Security Information Network (HISN)," Department of Homeland Security, at: http://www.dhs.gov/homeland-security-information-network-hsin, accessed December 31, 2014.

sharing network and $231 million spent, the program was only being used regularly by a fraction of the universe of federal, state, and local officials and law enforcement representatives who were intended to benefit from DHS's information sharing network.[78] The DHS Inspector General found that the HSIN had "35,560 active account holders nationwide," as of October 2012, but that only 4 percent of these users logged in to the system on a daily basis.[79] Only 12 percent, or roughly 4,270 people, checked the system at least once a week.[80] Among the reasons for the network's limited use cited by state and local officials was that "the system content was not useful."[81]

Besides these information sharing mechanisms, DHS's intelligence mission was also intended to provide utility for the federal government, state and local partners, and the private sector by conducting analysis and reporting useful information and assessments about security risks, including terrorism threats. But evidence casts doubt about the usefulness of the Department's Office of Intelligence and Analysis (I&A) and its intelligence products. For example, an analysis conducted by the Senate Select Committee on Intelligence found that in 2013, DHS had more analysts than finished intelligence products, meaning that DHS I&A produced less than one product per analyst that year.[82] A June 2014 report by the Government Accountability Office (GAO) raised additional questions about the usefulness of the intelligence that the DHS Office of Intelligence and Analysis's does produce. Surveys revealed that three key groups that I&A envisions to be the customers of its intelligence products—specifically, DHS's components, the Intelligence Community, and private critical infrastructure sector—did not find I&A's products to be useful.[83] GAO reported that the Department's own components, for example, "generally stated that they did not consider themselves customers of I&A with regard to finished intelligence products."[84]

---

[78] Department of Homeland Security Office of Inspector General, "Homeland Security Information Network Improvements and Challenges," OIG 13-98, June, 2013.
[79] Ibid, p.15-16.
[80] Ibid, p.16.
[81] Ibid, p.17.
[82] Opening Statement of Senator Tom Coburn, Senate Homeland Security and Governmental Affairs Committee, "Hearing on the Nominations of L. Reginald Brothers, Jr., to be Under Secretary of Science and Technology, U.S. Department of Homeland Security, and Hon. Francis X. Taylor to be Under Secretary of Intelligence and Analysis, U.S. Department of Homeland Security," March 5, 2014.
[83] Government Accountability Office, "DHS Intelligence Analysis: Additional Actions Needed to Address Analytic Priorities and Workforce Challenges," GAO 14-397, June 2014.
[84] Ibid, p.21.

The DHS Office of Intelligence and Analysis is fortunate to have a qualified and capable leader in General Francis X. Taylor serving as its Under Secretary for Intelligence and Analysis. Over the past year, General Taylor has begun to review and reform DHS I&A's programs and products. However, it remains to be seen whether DHS I&A can usefully serve its intended customers or provide a significant contribution to the nation's counterterrorism effort. The Department's intelligence initiatives should remain a focus of ongoing Congressional oversight.

DHS Grant Spending Subsidized State and Local Governments, But Provides Unknown Value to the Nation's Counterterrorism Effort

Another way that DHS has attempted to improve the nation's ability to prevent or respond to terrorism is through homeland security grants. FEMA provides state and local governments with preparedness program funding in the form of Non-Disaster Grants to enhance the capacity of state and local emergency responders to prevent, respond to, and recover from a weapons of mass destruction terrorism incident involving chemical, biological, radiological, nuclear, and explosive devices and cyber-attacks. Since 2003, DHS has spent more than $38 billion on preparedness grants.[85]

Independent reviews of DHS's preparedness programs, and their use by states and localities, reveal that DHS is not effectively managing this spending and ensuring that grant recipients are using funds to buy down risk and significantly improve our ability to prevent or recover from terrorist attacks. A June 2012 report by the DHS Office of Inspector General reported that "FEMA did not have a system in place to determine the extent that Homeland Security Grant Program funds enhanced the states' capabilities to prevent, deter, respond to, and recover from terrorist attacks, major disasters, and other emergencies before awarding more funds to the states."[86] In 2012, GAO reported on DHS's struggle to effectively manage the grant programs, finding that the Department "first developed plans in 2004 to measure preparedness by assessing capabilities, but these efforts have been repeatedly delayed." This hinders the Department's ability to ensure that grants are prioritized and used effectively to improve the

[85]Federal Emergency Management Agency, National Award Summary Report Data as of May 15, 2014.
[86] Department of Homeland Security Office of Inspector General, "The Federal Emergency Management Agency's Requirements for Reporting Homeland Security Grant Program Achievements," OIG 12-92, June 27, 2012, p.1.

nation's preparedness.[87] That year, GAO also reported that DHS needed to improve its coordination with four of the different grant programs to prevent the risk of duplication, including federal dollars being given to a state or locality twice for the same project.[88] Oversight raises questions about how states and localities are using DHS's homeland security grant funds.

In December 2012, Senator Coburn released a report, *Safety at Any Price: Assessing the Impact of Homeland Security Spending in U.S. Cities*, which reviewed states' and localities' use of preparedness grants.[89] The report identified many examples of states and localities making questionable purchases with homeland security grant funds. Tulsa, Oklahoma used Urban Areas Security Initiative (UASI) grant funding to harden a county jail and purchase a color printer.[90] Columbus, Ohio used DHS grant funds to purchase an underwater robot.[91] UASI funding was also used to pay first responders to attend a five day spa junket.[92] A community in Arizona used grant funding to install bollards and surveillance equipment at a spring training baseball stadium. Pittsburg, Pennsylvania used DHS grant funding to purchase a long-range acoustic device, a machine which emits an ear-splitting sound.[93] Many communities used DHS grant funding to purchase armored vehicles.[94]

At the time, the Senator Coburn's oversight report warned that one of DHS's grant programs, the Urban Areas Security Initiative, was transforming into an entitlement program for states and cities, and that the Department was effectively subsidizing state and local government's public safety expenditures, which creates a significant potential for waste in how these funds are spent.[95] A decision that contributed to this concern was DHS's change in policy in 2012 to streamline the grant process to improve states' and localities' ability to "put available

[87] Government Accountability Office, "Managing Preparedness Grants and Assessing National Capabilities: Continuing Challenges Impede FEMA's Progress," GAO-12-526T, March 20, 2012, highlights page.
[88] Government Accountability Office, "DHS Needs Better Project Information and Coordination among Four Overlapping Grant Programs," GAO-12-303, February 28, 2012.
[89] "Safety at Any Price: Assessing the Impact of Homeland Security Spending in U.S. Cities," A Report by Senator Tom Coburn, Homeland Security and Governmental Affairs Committee, December 2012.
[90] Ibid.
[91] Ibid.
[92] Ibid.
[93] Ibid.
[94] Ibid.
[95] Ibid.

funding to work now."[96] As of 2012, $8.3 billion of previously awarded grant funds remained unspent. Ironically, a key reason why DHS and FEMA made this decision to give states greater flexibility to put funding to use was "the current economic situation and the need for further fiscal stimulus."[97] Economic recovery is not a mission of DHS.

Countering Violent Extremism

One area where DHS may be more uniquely positioned to contribute to the nation's counterterrorism mission is in the federal, state, and local effort to counter violent extremism (CVE). In 2011, President Obama announced a national strategy for countering violent extremism, which included enhancing federal engagement efforts, strengthening government and law enforcement expertise, and countering extremist propaganda.[98] As a civilian agency charged with engaging with state and local law enforcement, as well as the private sector, DHS is better positioned to take a lead role providing training and engaging with community groups than other federal law enforcement or intelligence community agencies. A 2014 analysis by the Congressional Research Service of federal CVE initiatives identified DHS as the lead agency for the federal government in more than two-thirds of the activities and efforts discussed in the White House's plan.[99] In 2012, GAO reviewed DHS's and the Department of Justice's work establishing CVE training programs, and found that DHS was further along and more successful at that time than DOJ.[100]

However, GAO's analysis raised some questions about the training programs that DHS and DOJ were providing. "The majority of state and local participant feedback on [CVE-related] training that DHS or DOJ provided or funded," GAO reported, "was positive or neutral, but a minority of participants raised concerns about biased, inaccurate, or offensive material."[101] Given the nature of countering violent extremism initiatives and training, DHS and any other

[96] Department of Homeland Security, Grant Programs Directorate, "Guidance to State Administrative Agencies to Expedite the Expenditure of Certain DHS/FEMA Grant Funding," February 13, 2012, at: http://www.fema.gov/pdf/government/grant/grant_guidance_021312.pdf, accessed December 29, 2014, p.2.
[97] Ibid.
[98] "Strategic Implementation Plan for Empowering Local Partners to Prevent Violent Extremism in the United States," The White House, December 2011.
[99] Jerome P. Bjelopera, "Countering Violent Extremism in the United States," Congressional Research Service, February 19, 2014, p. 20.
[100] Government Accountability Office, "Countering Violent Extremism: Additional Actions Could Strengthen Training Efforts," GAO-13-79, October 18, 2012.
[101] Ibid.

federal entity engaged in this work will face a range of challenges, including how to most effectively engage with religious communities, including the Muslim community, and discuss or encourage law enforcement and community engagement with people who are involved in activities protected under the First Amendment of the Constitution. DHS's initiatives for countering violent extremism should remain a priority for oversight and Congressional review moving forward.

Private Sector Critical Infrastructure Initiatives

One of DHS's principle responsibilities is supporting critical infrastructure protection, including assets and systems whose destruction would have a debilitating impact on the nation's security, economy, health and safety. Since the private sector owns the majority of the nation's critical infrastructure, and these assets are spread across sectors of the economy that in some cases fall under the jurisdiction of other federal agencies, DHS and multiple federal agencies are involved in assessing risks, working with the private sector to address or mitigate them, and in some cases overseeing specific regulatory programs. Much of DHS's work related to infrastructure protection is conducted by the National Protection and Programs Directorate (NPPD), which is led by Under Secretary Suzanne Spaulding.[102]

Oversight of DHS's work related to private sector critical infrastructure assessments raises questions about how priorities are set and resources are used to help improve private sector security. For example, GAO reviewed DHS's programs for overseeing critical infrastructure from 2011 to 2013—including thousands of vulnerability assessments—and found significant variations in how DHS inspected or assessed critical infrastructure assets, which hinders DHS's ability to make comparisons and judgments about vulnerabilities and what should be prioritized.[103]

Given that the private sector owns the majority of the nation's critical infrastructure, DHS's success in its critical infrastructure protection mission largely depends on whether it can

[102] "Chairman Carper, Ranking Member Coburn Commend Senate n Confirmation of Critical DHS Leadership," Senate Homeland Security and Governmental Affairs Committee," March 6, 2014.
[103] Part of the challenge is that critical infrastructure inspection and assessments were being conducted by several different components and offices across DHS, yet the Department does not have standard guidance for what assessments should include or integrated systems or mechanisms for capturing and comparing data. See: Government Accountability Office, "Critical Infrastructure Protection: DHS Action Needed to Enhance Integration and Coordination of Vulnerability Assessment Efforts," GAO-14-507, September 15, 2014.

be a cooperative and efficient partner. Coordination and information sharing is a key aspect of any partnership with the private sector. In 2011, the Appropriations Committees of the Congress instructed DHS to review its efforts to streamline processes for coordinating and sharing information with private sector partners, including owners and operators of critical infrastructure, and to report on these efforts to Congress within 60 days.[104] Two years later, the Appropriations Committees' request was answered with a report from DHS. GAO reviewed the report and found it did "not discuss NPPD's effort to streamline the process for coordination and information sharing with industry partners," raising questions about whether the Department was responding to Congress and making progress in this respect to become a more efficient partner with the private sector.[105]

Protecting Against Domestic Chemical Biological, Radiological, and Nuclear Attacks

An important aspect of the Department's counterterrorism and domestic security responsibilities is to work to prevent domestic chemical, biological, radiological, nuclear, and explosive (CBRNE) attacks. Past chemical and biological attacks at home and abroad have demonstrated the potential for such attacks to kill, disrupt, and incite terror.[106] In the fall of 2001, Americans were terrorized by the use of bioweapons when letters containing anthrax were sent to media outlets and congressional offices, resulting in five deaths and significant disruption.[107] A terrorist attack detonating even a small scale nuclear device could lead to significant death and destruction. Similarly, a dirty bomb that exposed an area to radiological material would cause fear, panic, and destruction of property.[108]

Efforts to prevent the execution of such an attack are largely the responsibility of intelligence and law enforcement agencies; however, DHS's responsibilities in preventing CBRNE attacks largely focus on encouraging efforts to oversee and secure materials that could be used in such an attack, or to create and deploy tools to detect them before they are used. The

[104] Government Accountability Office, "Critical Infrastructure: Assessment of the Department of Homeland Security's Results of Its Critical Infrastructure Partnership Streamlining Efforts," GAO-14-100R, November 18, 2013.
[105] Ibid, p.3.
[106] For example, in 1995, a religious group conducted a coordinated biological attack releasing sarin gas in the Tokyo subway system, killing 13 and injuring or affecting thousands more. Melissa Locker, "Tokyo Sarin Gas Suspect Arrested, 17 Years Later," Time, June 4, 2012.
[107] "Amerithrax or Anthrax Investigation," Federal Bureau of Investigation, at: http://www.fbi.gov/about-us/history/famous-cases/anthrax-amerithrax, accessed December 31, 2014.
[108] For more information, see: "Fact Sheet on Dirty Bombs," United States Nuclear Regulatory Commission, at: http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/fs-dirty-bombs.html, accessed December 29, 2014.

agency has struggled in both areas, raising questions about whether the resources that taxpayers have spent on CBRNE security and detection initiatives and tools have yielded significant security enhancement and whether the nation is vulnerable to a catastrophic attack.

The history of the Department's key biosecurity programs highlight the challenge and mixed track record it has had in this work. In 2003, DHS launched the BioWatch program, which was intended to deploy machines to public areas to be able to detect early indications of a biological or chemical attack against the public.[109] Over the following eleven years, DHS spent approximately $1.1 billion on deploying and operating BioWatch.[110]

But there are open questions about whether BioWatch is an effective technology, given concerns about the number of false positives and negatives that have been reported,[111] as well as whether the technology effectively detects biological attacks in time to respond to a potential attack. In other words, the program may not always detect a real biological attack, and what it does warn of are not biological attacks.

In 2011, the Institute of Medicine and the National Research Council of the National Academies reviewed the BioWatch program at the request of DHS.[112] The reviewers identified significant problems with the program, including the need for "better technical and operational testing to establish its effectiveness," and raised questions about whether the program was an effective use of resources, since the annualized cost of the program would be $80 million annually as of 2011 or as much as $200 million if a Generation 3 BioWatch system was deployed.[113] The Institute of Medicine and the National Research Council of the National Academies recommended that DHS reassess the program; specifically that is should assess "its effectiveness and frame program goals from a risk-management perspective" and "conduct systematic operational testing of current and proposed BioWatch technologies."[114]

---

[109] Dana A. Shea and Sarah A. Lister, "The BioWatch Program: Detection of Bioterrorism," Congressional Research Service, November 19, 2003.
[110] David Willman, "Homeland Security cancels plans for new BioWatch technology," Los Angeles Times, April 25, 2014.
[111] For example, the Los Angeles Times reported that the BioWatch system had experienced 56 BioWatch false alarms between 2003 and 2008. See: David Willman, "The biodefender that cries wolf," The Los Angeles Times, July 8, 2012.
[112] Institute of Medicine and the National Research Council of the National Academis, "BioWatch and Public Health Surveillance: Evaluating Systems for the Early Detection of Biological Threats: Abbreviated Version," 2011.
[113] Ibid, p.1-2.
[114] Ibid, p.2.

In 2014, following a GAO-recommended analysis of alternatives, DHS canceled its plans to acquire and deploy Generation 3 BioWatch technologies after spending $61 million between 2008 and 2013 on the project.[115] The move, however, saved taxpayers an estimated additional $5.7 billion originally planned for Generation 3.[116] Given the open questions about the feasibility and the cost-effectiveness of the project, the decision to cancel the project was smart. However, it does not address whether continuing to operate the existing generation BioWatch system is a valuable use of resources or makes the nation safer from potential biological or chemical attack.[117] Given the processing time for existing BioWatch equipment, traditional biosurveillance (including hospitals and labs) would likely detect an attack before BioWatch, meaning the money spent on the current iteration of BioWatch might be better spent enhancing existing, traditional biosurveillance tools.

DHS has also faced challenges over the past decade developing and deploying cost-effective systems for detecting nuclear or radiological matter, including for scanning cargo entering the country. In 2005, the President established the Domestic Nuclear Detection Office (DNDO) within DHS for the purpose of acquiring and supporting deployment of radiation detection equipment.[118] In September 2010, the Senate Homeland Security and Governmental Affairs Committee held a hearing to examine the state of DHS's programs for detecting smuggled nuclear material, after spending $4 billion on the project over the five year period.[119] At the hearing, Senator Joe Lieberman and Senator Susan Collins, then chairman and ranking member respectively, expressed disappointment with DNDO's inability to create a strategic plan for nuclear smuggling detection efforts and with the failure of DNDO's two largest technology projects.[120] One of these projects was the acquisition and deployment of advanced spectroscopic portals (ASP) for detecting nuclear material. In 2011, the National Academies of Sciences reviewed DHS's management of the ASP project and identified widespread problems,

[115] Jared Serbu, "DHS cancels $6 billion program to detect bioweapons, with no Plan B," June 11, 2014.
[116] Ibid.
[117] GAO analyzed the decision to cancel BioWatch Generation 3 project and found that the decision to cancel the project "raises potential challenges" for the currently deployed Gen-2 system," given questions about the technology's effectiveness and the need to replace some of the Gen-2 systems equipment moving forward. Government Accountability Office, "Observations on the Cancelation of BioWatch Gen-3 and Future Considerations of the Program," GAO-14-267T, June 10, 2014.
[118] Testimony of DHS DNDO Director Warren Stern, House Committee on Homeland Security, Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, September 10, 2010.
[119] "Senators Strafe DHS for Nuclear Detection Program Failures; GAO Accuses DHS of 'Misleading' Congress," Committee on Homeland Security and Governmental Affairs, September 15, 2010.
[120] Ibid.

including shortcomings in the tests that "impair DHS'[s] ability to draw reliable conclusions about the ASP's likely performance."[121] In October 2011, DHS canceled the ASP monitor program for radiation screening after the equipment failed a series of field validation tests.[122] By that point, DHS had already spent $230 million developing the machines.[123]

There are scientific and practical challenges associated with developing and deploying cost-effective technologies to detect potential chemical, biological, radiological, and nuclear threats. But the past twelve years, and multiple reviews by watchdogs and scientific experts, suggests that the billions that DHS has spent on CBRNE detection systems have not yielded commensurate improvements in our nation's ability to prevent CBRNE terrorist attacks, raising the question of whether DHS is equipped to successfully execute its responsibilities in this area and whether taxpayer funding devoted to these efforts may be put to better use in other areas that create measurable security enhancements.

Chemical Facility Security (CFATS)

A case study of DHS's efforts to secure private sector critical infrastructure is the Chemical Facilities Anti-Terrorism Standards (CFATS) program, which is managed by the Department's National Protection Program Directorate (NPPD).[124] Chemical facilities present a target of opportunity for would-be terrorists if left unsecured, as the nation has seen with past attempts to blow up chemical facilities, including one of the nation's largest propane facilities.[125] In 2006, Congress authorized the Department to work to secure chemical facilities across the country under CFATS.[126] Since then, the Department has spent $595 million and hired 250 personnel to launch a regulatory and inspection program, develop security standards for chemical facilities, as well as analyze and determine which chemical facilities present the greatest risk.[127]

---

[121] National Research Council of the National Academies, "Evaluating Testing Costs, and Benefits of Advanced Spectroscopic Portals: Final Report," 2011, p. 2.
[122] Government Accountability Office, "Combating Nuclear Smuggling: Lessons Learned from Canceled Radiation Portal Monitor Program Could Help Future Acquisitions," GAO-13-256, May 2013.
[123] Noel Brinkerhoff, "Homeland Security Cancels $230 Million Radiation Detection Program," AllGov.com, July 28, 2011.
[124] Ibid.
[125] "Police: California Men Planned to Bomb Propane Tanks," CNN.com, Dec. 4, 1999.
[126] Senator Tom Coburn, "Chemical Insecurity: An Assessment of Efforts to Secure the Nation's Chemical Facilities from Terrorist Threats," U.S. Senate Homeland Security and Governmental Affairs Committee, July 2014.
[127] Ibid.

In July, Senator Tom Coburn released a report presenting the findings of a yearlong investigation into the CFATS program.[128] The investigation identified significant problems, including that CFATS is not reducing the risk of a terrorist attack on domestic chemical infrastructure, and DHS does not know whether some dangerous chemical facilities exist.

Senator Coburn's investigation also revealed that the Department is failing to meet key deadlines, validate security plans, or conduct compliance inspections established by the CFATS program. For example, as of July 2014, 99 percent of all CFATS regulated facilities had never been inspected by DHS for compliance in the program's eight years of existence, and 78 percent of CFATS regulated facilities still have not had their security plans approved by DHS.[129] While doing little to reduce risk, CFATS is costly to the companies it regulates, as it requires many small businesses to submit thousands of pages in forms and paperwork, and in some cases requires facilities to resubmit paperwork and forms that DHS takes several years to process and review.[130]

The CFATS program, and DHS's struggle to effectively establish and enforce security standards and regulations for chemical facilities over eight years after spending more than a half a billion dollars, provides a cautionary note about DHS's historical ineffectiveness in the area of critical infrastructure security regulations and enforcement.

DHS Programs to Protect Federal Buildings

DHS also has certain key responsibilities for protecting federal facilities. The importance of this job was highlighted in October 2014 when Secretary Jeh Johnson announced an initiative to enhance the presence of DHS's Federal Protective Service (FPS) at government buildings as a "precautionary step" given the current threat environment.[131] That federal buildings are target of terrorism and other violence was made clear to the nation nearly twenty years ago with the horrific terrorist attack against the Alfred Murrah building in Oklahoma City, Oklahoma. Recent evidence has underscored the threat, including attacks at home and abroad, such as the

[128] Ibid.
[129] Ibid.
[130] Ibid.
[131] "Statement by Secretary Johnson on Enhanced Presence of the Federal Protective Service at U.S. Government Buildings in the United States," Department of Homeland Security, October 28, 2014.

2013 shooting at the Washington Navy Yard facility and the 2014 shooting at the Canadian Parliament.

The Federal Protective Service, which is managed by DHS's National Protection Program Directorate (NPPD), is comprised of more than 1,300 federal employees and uses a workforce of roughly 13,000 contract employees to secure the government's 9,500 federal facilities.[132] Both GAO and the Inspector General identified challenges facing the FPS and questions about its ability to secure federal facilities and protect the public and employees there. Repeated GAO audits have found that DHS struggles to ensure that its contracted security officers have the necessary training and certifications. For example, in 2013, GAO reported that one contract security company that FPS uses reported that 38 percent of its guards did not receive training to use X-ray and magnetometer screening from FPS, which is the process for screening people for weapons or explosives entering a building, and some officers who did not receive this training were working at screening posts.[133] In 2014, GAO reported that FPS still is not providing training for how to respond to an active shooter scenario.[134]

The Inspector General also identified problems with FPS's performance, including one alarming example that raised questions about whether some of FPS's employees or contract guards are prepared to mitigate or even recognize a potential bombing attack. A Department of Homeland Security OIG Report issued in August 2012 reviewed an incident at the Patrick V. McNamara Federal Building in Detroit. Contract security officers found a bag containing an improvised explosive device outside of the building. The guards brought the bag, which contained a locked safe, inside the building. They attempted to determine the contents of the bag by "shaking and moving the metal safe inside the bag," which contained the IED, and X-raying the bag.[135] The Inspector General reports that the security guards placed the bag and its contents at their security console for a period of 21 days.[136] The report noted that the guards

[132] "Federal Protective Service operations," Department of Homeland Security, at http://www.dhs.gov/fps-operations, accessed December 29, 2014.
[133] Government Accountability Office, "Challenges Associated with Federal Protective Services' Contract Guards and Risk Assessments at Federal Facilities," GAO-14-128T, October 30, 2013.
[134] "According to officials at five guard companies, their contract guards have not received training or how to respond during incidents involving an active shooter," which, GAO warned, means that DHS and FPS have "limited assurance that its guards are prepared for this threat." Government Accountability Office, "Federal Protective Service: Protecting Federal Facilities Remains a Challenge," GAO-14-623T, May 21, 2014.
[135] Department of Homeland Security Office of Inspector General, "Effects of a Security Lapse on FPS' Michigan Guards Services Contract," OIG-12-100 (Revised), August 2012, p.6.
[136] Ibid.

were working with equipment they did not know how to use, procedures for handling found property were unclear, and FPS post inspections did not identify unauthorized items at the post.[137]

Security of the White House and Presidential Protection

Another responsibility within DHS's domestic security mission is to secure and protect the White House, the President, and other national leaders. This responsibility largely falls to the United States Secret Service (USSS), a component whose history began nearly a century and a half before DHS was created.[138] But recent events suggest that there are areas of improvement that the U.S. Secret Service must address to successfully execute its responsibilities for securing the White House, President Obama and his family, and other national leaders.

A September 2014 incident revealed a potential weakness in the USSS's protection of the President and the White House complex. On September 19, 2014, a man jumped the White House fence, defeated the perimeter security on the grounds, entered the White House building through an unlocked door, evaded the capture of a USSS officer upon entry, and traveled into the White House building where he came dangerously close to a staircase that leads to the First Family's residence before being tackled and captured.[139]

The September incident was the most recent of a series of security lapses that have occurred during President Obama's administration,[140] including a serious attack against the White House that occurred in 2011 and involved the shooting of a semiautomatic rifle at the White House,[141] a breach of security standards in 2009 when two reality TV personalities crashed a White House State Dinner without invitations or identification, and a December 2013 incident when an imposter sign language translator who had faced past charges of rape and murder gained close access to President Obama while he spoke at Nelson Mandela's memorial service.[142]

---

[137] Ibid.
[138] "Secret Service History," U.S. Secret Service, Department of Homeland Security, at: http://www.secretservice.gov/history.shtml, accessed December 31, 2014.
[139] Carol D. Leonnig, "White House fence-jumper made it far deeper into building than previously known," Washington Post, September 29, 2014.
[140] "Secret Service Blunders Continued Under Pierson," Wall Street Journal, October 1, 2014.
[141] Carol D. Leonnig, "Secret Service fumbled response after gunman hit White House residence in 2011," The Washington Post, September 27, 2014.
[142] "Secret Service Blunders Continued Under Pierson," Wall Street Journal, October 1, 2014.

Shortly after the September 2014, Secretary Johnson created a panel led by Deputy Secretary Mayorkas to investigate and report on the breach of the White House. The report was released in November and outlined systemic failures by the USSS to identify and monitor the suspect as a threat to the White House. Intelligence, investigative, communications, operational and management failures were identified in the report.[143] In December 2014, an independent panel issued a report requested by Secretary Jeh Johnson. The panel reported that the Secret Service is "an organization starved for leadership that rewards innovation and excellence and demands accountability."[144]

The U.S. Secret Service faces broad questions about how it should strengthen its workforce, culture, and improve its performance.[145] Some have even questioned whether the Secret Service's inclusion in the Department of Homeland Security has contributed to its problems and challenges executing its mission.[146] The recent security lapses and the problems identified by the various audits and reviews suggest that DHS and the USSS must do better to ensure that the Department succeeds in its essential responsibility to protect President Obama, his family, other national leaders, and the White House.[147]

Conclusion

A review of DHS's counterterrorism and domestic security initiatives raises a series of questions about the value and effectiveness of DHS's programs. It is not clear that the DHS programs designed to prevent terrorist attacks—including its intelligence, information sharing,

[143] "Executive Summary of the U.S. Department of Homeland Security Report on the White House Incursion Incident of September 19, 2014," Department of Homeland Security, November 13, 2014.
[144] Joseph Hagin, Thomas Perrelli, Danielle Gray, Mark Filip, United States Secret Service Protective Mission Panel, "Executive Summary to Report from the United States Secret Service Protective Mission Panel to the Secretary of Homeland Security," December 15, 2014.
[145] For example, a 2013 survey by the Office of Inspector General found that only 61 percent of USSS employees that responded to the survey "believed management does not tolerate misconduct," suggesting that nearly four out of ten USSS employees responding to the survey did believe that misconduct was tolerated. DHS Office of Inspector General, "Adequacy of USSS Efforts to Identify, Mitigate, and Address Instances of Misconduct and Inappropriate Behavior (Redacted)," OIG-14-20, December 2013, p.1.
[146] Carol D. Leonnig, "Critical decisions after 9/11 led to slow, steady decline in quality for Secret Service," The Washington Post, December 27, 2014.
[147] The United States Secret Service Protective Mission Panel warned, "The paramount mission of the United States Secret Service—protecting the President and other high-ranking national officials—allows no tolerance for error. A single miscue, or even a split-second delay, could have disastrous consequences for the Nation and the world." See: Joseph Hagin, Thomas Perrelli, Danielle Gray, Mark Filip, United States Secret Service Protective Mission Panel, "Executive Summary to Report from the United States Secret Service Protective Mission Panel to the Secretary of Homeland Security," December 15, 2014, p.1.

and preparedness grants programs—are making the nation safer or accomplishing DHS's stated priority mission. Likewise, DHS's initiatives aimed at improving domestic security from potential terrorist attacks have a history of problems, and there are questions about their effectiveness or utility. DHS's technology initiatives and programs designed to monitor and detect chemical, biological, radiological, or nuclear attacks have not proven to be effective or cost-efficient, and billions of dollars have been spent on these initiatives. DHS has similarly struggled with its responsibilities for identifying and prioritizing critical infrastructure protection, including spending eight years and more than half a billion dollars on a program to secure chemical facilities which has yielded few tangible results. DHS has even struggled to effectively manage its responsibilities for securing federal facilities and protecting the President of the United States.

Given the importance of the nation's counterterrorism and protective security missions, Congress and the Department should review and reconsider DHS's programs related to its first mission—ending programs and initiatives that are non-essential or yielding few improvements in enhanced security. Congress and DHS's leadership must reconsider how DHS can provide a more significant contribution to the nation's counterterrorism mission. Moreover, DHS must ensure that it is executing its critical protective security responsibilities, including protecting the President and other national leaders.

Mission 2— Securing and Managing Our Borders

Overview

The Department's second mission is "securing and managing our nation's borders." According to the Department's current strategy, achieving this mission involves accomplishing "three interrelated goals: effectively securing U.S. air, land, and sea borders; safeguarding and streamlining lawful trade and travel; and disrupting and dismantling transnational criminal and terrorist organizations."[148]

In 2014, the challenge and necessity of securing the United States' land, sea, and air borders was highlighted by destabilizing and unexpected events both here and abroad, including the continued mass migration to our Southern border and the emergence of potential terrorism and public health threats. The number of illegal immigrants—including those known as unaccompanied alien children (UACs)—arriving at our Southern border and surrendering to federal authorities was approximately 68,000 as of November 2014, nearly double the 38,000 in 2013.[149] This created a daunting logistical challenge for DHS, as well as other federal agencies, requiring the redirecting of resources from securing the border to processing and caring for arriving children and families.[150]

Concern also mounted in October over the potential risk to public health associated with a dramatic increase in mass migration to the Southern border if the Ebola virus reached Central America. Marine Corps General John F. Kelly, the commander of U.S. Southern Command (SOUTHCOM), warned about the consequences of an Ebola outbreak spreading to Central America. As he put it, "If it breaks out, it is literally, 'Katie bar the door', and there will

[148] "Department of Homeland Security Strategic Plan: Fiscal Years 2012-2016," Department of Homeland Security, February 2012.
[149] "Southwest Border Unaccompanied Children," The Department of Homeland Security, U.S. Customs and Border Protection: Newsroom, at: http://www.cbp.gov/newsroom/stats/southwest-border-unaccompanied-children, accessed December 29, 2014.
[150] For a thorough discussion of the challenges associated with the Unaccompanied Alien Children problem, see this analysis by the Congressional Research Service: Lisa Seghetti, et all, "Unaccompanied Alien Children: An Overview," Congressional Research Service, September 8, 2014. The Senate Homeland Security and Governmental Affairs Committee also held a hearing examining the challenges associated with the UAC crisis on July 9, 2014.

be mass migration into the United States. They will run away from Ebola, or if they suspected they are infected, they will try to get to the United States for treatment."[151]

Further, some elected officials have voiced concerns about the potential for Islamic extremists plotting terrorist attacks to seek entry across either the Southern or Northern borders.[152] There are also concerns that some of the thousands of Westerners currently in Syria and Iraq as foreign fighters, including U.S. citizens, have been exposed to an environment of sustained radicalization, and could come to America, using Western passports, intent on committing acts of terrorism.[153]

These disconcerting issues raise a basic question: how effectively is the United States securing our borders and ports of entry? For several years, DHS leaders and senior officials have told Congress and the American people about improvements that have been made by the Department to ensure our nation's borders are more secure than ever. In 2011, for example, former Secretary Napolitano told the public that "the border is better now than it has ever been."[154] In testimony before the Senate Homeland Security and Governmental Affairs Committee, she asserted that the "Administration has dedicated more resources to securing the Southwest border than ever before, in terms of manpower, technology, and infrastructure," and that "progress has been made" as a result.[155] In 2013, senior DHS officials testifying before the Committee also stated "the border is more secure than ever before"[156] and that the Department "has undertaken an unprecedented effort to secure our border."[157]

---

[151]Jim Garamone, "Kelly: Southcom Keeps Watch on Ebola Situation," DoD News, Defense Media Activity, October 8, 2014.

[152] In 2011, Senator Lieberman and Senator Collins of the Senate Homeland Security and Governmental Affairs Committee raised concerns about the potential for terrorists to gain entry across the Northern border. See: Jack Cloherty and Pierre Thomas, "Congress: Border with Canada the Weak Link in Terror Security," ABC News, February 1, 2011. In 2014, Texas Governor Rick Perry was one of several elected officials to raise concerns about terrorists, including the Islamic State, seeking to gain entry into the country through vulnerabilities in our Southern border security. See: Ashley Killough, "Rick Perry: It is possible ISIS has crossed the Southern border," CNN, August 21, 2014.

[153] See: "Cybersecurity, Terrorism, and Beyond: Addressing Evolving Threats to the Homeland," Senate Homeland Security and Governmental Affairs Committee Hearing, September 10, 2014.

[154]Jennifer Epstein, "Janet Napolitano: Border security better than ever," Politico, March 25, 2011.

[155]Testimony of Secretary Janet Napolitano Before the U.S. Senate Homeland Security and Governmental Affairs Committee, May 4, 2011.

[156]Testimony of Randolph Alles (Assistant Commissioner Office of Air and Marine), Michael J. Fisher (Chief, U.S. Border Patrol), Kevin McAleenan (Acting Deputy Commissioner, U.S. Customs and Border Protection) Before the Senate Committee on Homeland Security and Governmental Affairs, April 10, 2013.

[157] Ibid.

It is true that more resources than ever have been devoted to DHS's border security initiatives. According to the Congressional Research Service, taxpayer spending on Customs and Border Protection's border security programs totaled more than $85 billion between 2006 and 2013.[158] However, this does not ensure that the border is effectively controlled or that the risk of people illegally crossing our borders has been significantly reduced. Documents made available to the Homeland Security and Governmental Affairs Committee reveal that gaps in border security along the Southern Border span more than 700 miles where there is little to no deployment density or aviation surveillance coverage.[159] Moreover, thousands of miles of the Northern border with Canada, where there are few if any resources deployed to secure the border, are also uncontrolled.[160]

With these broad gaps in coverage of both our Southern and Northern borders, the problem of people and goods illegally entering our country remains a significant concern, and a committed adversary seeking illegal entry into the United States has a reasonable chance of doing so undetected. For example, experts writing for the Council on Foreign Relations in 2013 estimated that the apprehension rate along our Southwest border is 40 to 55 percent.[161]

DHS's secondary objectives for securing and managing our borders—securing air and sea borders, safeguarding trade and travel, and disrupting and dismantling international criminal and terrorist organizations—also present significant challenges. While our nation has not suffered a successful aviation security attack since 2001, there have been significant lapses in our air travel initiatives. A review of TSA's programs identifies several areas where the agency could improve its strategy and efficiency.[162] Likewise, DHS has not succeeded in its efforts to secure

---

[158] Lisa Seghetti and Jerome P. Bjelopera, Congressional Research Service, Memorandum to Senate Homeland Security and Governmental Affairs Committee, January 16, 2014.

[159]Committee minority staff review and analysis of documents provided by DHS and Customs and Border Protection.

[160]Ibid. This finding is consistent with past evidence about the state of security on the Northern border. For example, GAO reported in 2010 that only "32 of the nearly 4,000 northern border miles in fiscal year 2010 had reached an acceptable level of security." Government Accountability Office, Border Security: Enhanced DHS Oversight and Assessment of Interagency Coordination is Needed for the Northern Border, GAO-11-97, December 17, 2010.

[161]Bryan Roberts, Edward Alden, John Whitley, "Managing Illegal Immigration to the United States: How Effective is Enforcement?" Council on Foreign Relations, May 2013.

[162]Government Accountability Office, Aviation Security: TSA Should Limit Future Funding for Behavior Detection Activities, GAO-14-158T, November 14, 2013; Government Accountability Office, Advanced Imaging Technology: TSA Needs Additional Information before Procuring Next-Generation Systems, GAO-14-357,; Government Accountability Office, Homeland Security: DHS and TSA Continue to Face Challenges Developing and Acquiring Screening Technologies, GAO-13-469T, May 8, 2013.

U.S. port facilities, infrastructure, and incoming cargo from potential terrorist attacks, despite spending upward of $5 billion on these initiatives since 2002.[163]

Several of DHS's components, including Immigration and Customs Enforcement (ICE), U.S. Secret Service, and U.S. Coast Guard, have responsibilities concerning and are engaged in activities for disrupting international criminal or terrorist organizations. While they have demonstrated successes, this work is not the sole or primary responsibility of any of these components, raising questions about whether this Departmental objective is only aspirational, or is truly likely to be accomplished.

Are U.S. Borders Secure?

On October 9, 2014, Secretary Jeh Johnson delivered a speech and presentation in Washington, D.C. presenting the Department's plans for "Border Security in the 21st Century."[164] Addressing the past, present, and future, Secretary Johnson stressed the growing resources that have been devoted to border security; including an increase from 8,617 Border Patrol agents on the Southern border in 2000 to 18,127 agents in 2014, and an increase from 77 miles of total fencing in 2000 to 700 miles of fencing today.[165] Secretary Johnson also highlighted other increases in assets deployed along the Southern border, including 70 miles of border lighting, 11,863 border sensors to detect illicit migration, 107 Border Patrol aircraft, 8 unmanned aerial vehicles (UAVs), 84 vessels patrolling waterways on the Southern Border, and other new surveillance tools.

Secretary Johnson pointed to declining numbers of apprehensions along the Southern border as an indicator of the Border Patrol's success controlling the border and deterring would-be trespassers. Specifically, he pointed to data showing that apprehensions totaled 479,000 for

---

[163]For background on the challenges DHS has faced with its port security initiatives, see: U.S. Senate Homeland Security and Governmental Affairs Committee Hearing: "Evaluating Port Security: Progress Made and Challenges Ahead." June 4, 2014. For the $5 billion estimate: According to information provided to the minority staff by DHS, the Department has spent approximately $5.167 billion on its various initiatives related to port security since 2002, including $2.958 billion on the Port Security Grant Program, 959 million on the Container Security Initiative, 411.9 million on the Customs-Trade Partnership Against Terrorism, 336.7 million on the Automated Targeting System, 60 million on the Secure Freight Initiative, $21.8 million on the Coast Guard's waterways and coastal security efforts, and $420 million on the Transportation Worker's Identification Credential. Committee staff analysis December 2014.

[164]Remarks by Secretary of Homeland Security Jeh Johnson at the Center for Strategic and International Studies, "Border Security in the 21st Century," October 9, 2014.

[165]Ibid.

FY 2014, in comparison to the roughly 1.6 million apprehensions in FY 2000.[166] The apprehensions figure for FY 2014 follows a three-year trend of steady increases in the number of apprehensions since FY 2011, when DHS data shows that Southern border apprehensions hit a low of 327,000.[167]

Based on the information that is available, it is impossible to judge whether the border is secure based on these statistics for several reasons. First, the data that DHS has made available, including apprehension rates, does not answer the question of whether the border is secure. The Department is not reporting so-called "got-aways" or people who have succeeded in crossing the border that are known to them. Nor can DHS report the number of people that got-away that it did not detect.[168] Second, statistical trends, such as increasing or declining numbers of apprehensions, are not an effective measure to judge the state of border security. Many other variables, including social and economic factors, such as the availability of jobs in the United States or in illegal immigrants' countries of origin, affect people's decisions about whether to seek illegal entry into the United States.[169] Third, historically, DHS has not been forthcoming or transparent in its reporting of border security statistics, hindering both policymakers' and the public's ability to carefully study data and understand potential trends.[170]

Understanding these limits, estimates about the overall effectiveness of border security, and specifically the chances of federal authorities stopping an illegal immigrant seeking entry along the Southern border, vary broadly. According to DHS and the Border Patrol, for example, the "effectiveness rate" in some sectors along the Southern border is approaching 80 to 85

---

[166] Ibid, slide 26.
[167] Ibid, slide 26.
[168] Members of the Senate Homeland Security and Governmental Affairs Committee have pointed out that it is impossible to judge the effectiveness of DHS's border security measures based on the number of apprehensions alone, since that measure does not include a calculation of how many illegal immigrants successfully gained entry to the United States. [For example, see Dr. Coburn's questions and comments about the denominator at the Senate Homeland Security and Governmental Affairs Committee's May 7, 2013 hearing on border security.] A significant decline in apprehensions could occur, hypothetically, if U.S. Border Patrol ceased its efforts to apprehend illegal border crossers and allowed all illegal immigrants to gain entry without being apprehended, which of course would not prove the success of DHS's security measures and deterrence.
[169] Bryan Roberts, Edward Alden, John Whitley, "Managing Illegal Immigration to the United States: How Effective is Enforcement?" Council on Foreign Relations, May 2013.
[170] In some instances, DHS has delayed the release of key information that Congress has mandated be provided. For example, DHS provided the Homeland Security and Governmental Affairs Committee its quarterly "Border Security Status Reports" for FY 2012 in December 2013, long after the data should have been collected, and only after Chairman Tom Carper co-signed a letter requesting it. To date, the Department has not yet provided or published its quarterly "Border Security Status Reports" for FY 2013 to the Senate Homeland Security and Governmental Affairs Committee.

percent.[171] In contrast, researchers writing for the Council on Foreign Relations estimated that a person trying to enter the country illegally along the Southern border overall had a 40 to 55 percent chance of getting caught or turned back.[172]

Lacking a clear statistical picture of apprehension rates and the number of people who enter the country illegally at our Southern or Northern borders, policymakers must look to other evidence to judge whether or not DHS is accomplishing its mission of securing the nation's borders. Senator Coburn sought to answer the question of how complete our border security is by requesting the Department's strategic plans for securing the Southern border, and by reviewing information related to its deployment of assets along the border and any gaps in coverage, its use of aerial assets to close coverage gaps, and other potential vulnerabilities within DHS's border defenses, including the potential for workforce corruption. In each of these areas, the evidence suggests that U.S. borders are not fully secure, and DHS cannot successfully prevent illegal immigrants or determined adversaries, including drug trafficking organizations, from gaining entry.

DHS Lacked a Department-Wide Border Security Plan Until 2014

Despite the fact that both the current National Security Strategy and the DHS Strategic Plan include border security strategy as a priority mission, the Department of Homeland Security apparently did not have a comprehensive, Department-wide strategy for border security and immigration enforcement until late in 2014. During the summer of 2013 and the legislative debate about S. 744 (the Border Security, Economic Opportunity, and Immigration Modernization Act), Senator Coburn requested that the Department make available to the Committee its strategy for securing the Southern border. DHS did not provide a comprehensive border security strategy.[173]

---

[171] Cory Kane, "Senators call border security the major hurdle in immigration reform," Houston Chronicle, May 7, 2013.

[172] This analysis was based in part on survey and recidivism data. Bryan Roberts, Edward Alden, John Whitley, "Managing Illegal Immigration to the United States: How Effective is Enforcement?" Council on Foreign Relations, May 2013.

[173] The documents that DHS did provide to the Committee did not amount to a Department-wide strategy and did not clearly detail coordination between components. For example, the Department provided the Border Patrol Strategic Plan: 2012 to 2016. However, this did not have detailed information about the Department's plans to secure the Southern border, but instead included a high-level overview of CBP's programs and activities. This document also included few references to other components that are involved in initiative that support or are essential to securing the Southern border. For example, this Border Patrol strategic plan does not reference

Senator Coburn and other members of the Committee continued to press DHS for information related to its border security strategy and outcome measures.[174] In a December 16, 2013 letter to four members of the Committee, DHS provided an explanation about the Department's process for setting components' mission and strategy, which indicates that the DHS Office of Policy plays a role in coordinating components' border security efforts. DHS stated that, "As it relates to the Department's cross-Component border security strategy, agencies are guided by a number of policies, internal strategies, and directives. The Department's Office of Policy and Office of Operations Coordination and Planning coordinate border security efforts among Departmental Components."[175]

However, a review of the publicly available strategic documents for several DHS components involved in border security and immigration enforcement reveals that these strategies are not strongly linked or aligned, and suggests that they were not closely coordinated or aligned with other components when they were developed.[176] In some cases, the DHS components' strategic documents were out of date.[177]

In 2014, DHS Secretary Jeh Johnson took action to ensure that the Department developed a comprehensive Southern border security strategy. His April 22, 2014 memorandum to DHS Leadership titled "Strengthening Departmental Unity of Effort" included a direction requiring the Deputy Secretary to oversee the development of a "strategic framework for the security of the U.S. Southern Border and approaches by August 1, 2014, along with a set of

---

Immigration and Customs Enforcement or Coast Guard. See: U.S. Customs and Border Protection, "2012-2016 Border Patrol Strategic Plan," Department of Homeland Security.

[174] Letter from Senator Carper, Senator Coburn, Senator McCain, and Senator Levin to the Honorable Rand Beers, Acting Secretary of the Department of Homeland Security, December 12, 2013.

[175] Letter from Acting Secretary Rand Beers to Senator Tom Coburn, December 16, 2013.

[176] See: U.S. Customs and Border Protection, *Secure Borders, Safe Travel, Legal Trade, Fiscal Year 2009 – 2014 Strategic Plan*, July 2009; U.S. Immigration and Customs Enforcement, *ICE Strategic Plan FY 2010 – 2014*, June 2010. There are some references to other components and collaboration in these strategic documents; however, they are limited and suggest that cross-component collaboration was not a key aspect of each components' or the Department's overall strategy. For example, CBP's strategy document includes the section described as "cross-cutting enablers" that directly or indirectly relate to the border security and immigration mission and how CBP intends to "evolve and strengthen" its partnerships with ICE, Coast Guard, and other DHS component to push toward gaining operational control of the border. But the CBP strategy includes few references to collaboration with ICE and USCG. The *ICE Strategic Plan, Fiscal Year 2010-2014*, lists several goals, and has some evidence of collaboration, though the vast majority of ICE's goals do not involve working with other stakeholders. Specifically, only 2 out of the 20 objectives listed in the ICE strategy include working with CBP.

[177] For example, see: USCIS Strategic Plan: 2008-2012, which expired in 2012 and had not been updated. Both the ICE and CBP strategic plans expired in 2014.

nested 'campaign plans' for specific geographic areas or problem sets."[178] An official from the U.S. Coast Guard was tasked with leading the plan's development.[179]

Large Gaps in Border Security Coverage Exists

A review of DHS's internal documents shows that there are significant gaps in border security coverage. DHS documents made available to the Homeland Security and Governmental Affairs Committee reveal that there is at least 700 miles of gaps in coverage along our Southern border, where there is little to no Border Patrol deployment density or aviation surveillance coverage.[180] In one Southern border sector, the border security gaps in coverage amounted to more than 70 percent of the sector.[181]

Border security coverage along the Northern border is even less dense than along the Southern border, suggesting that there is little or no border security coverage for thousands miles of the United States' Northern border with Canada.[182] This is consistent with past findings about the state of security on the Northern border. For example, GAO reported in 2010 that only "32 of the nearly 4,000 northern border miles in fiscal year 2010 had reached an acceptable level of security."[183]

DHS Has Struggled to Use Air Assets for Border Security Surveillance

One way that DHS could potentially address broad gaps in border security density and coverage would be to use aerial surveillance assets and technology. Yet, DHS has struggled to use its aerial surveillance assets. A review of documents provided by DHS and Customs and Border Protection shows that the Office of Air and Marine (OAM) struggles to effectively use its aerial surveillance equipment, which the Department relies on to provide border security coverage where fewer assets are deployed on the ground.

---

[178] Secretary Jeh Johnson, "Memorandum to DHS Leadership: Strengthening Departmental Unity of Effort," April 22, 2014.
[179] Ibid.
[180] Committee minority staff review and analysis of documents provided by DHS and Customs and Border Protection and DHS. Also, comments of Senator Tom Coburn, Senate Homeland Security and Governmental Affairs Committee Hearing, September 10, 2014.
[181] Committee minority staff review and analysis of documents provided by DHS and Customs and Border Protection and DHS.
[182] Ibid.
[183] Government Accountability Office, Border Security: Enhanced DHS Oversight and Assessment of Interagency Coordination is Needed for the Northern Border, GAO-11-97, December 17, 2010.

The problem of DHS's ineffective use of its existing aircraft has persisted over several years. In 2014, DHS told the Committee that its ten unmanned aerial vehicles flew a total of approximately 5,000 hours in 2013, suggesting that the vehicles flew for less than twelve hours per week.[184] One of the aerial assets that DHS used was only flown for approximately 7 hours per week in FY 2013.[185] In 2012, the DHS Office of Inspector General found that DHS's seven Unmanned Aircraft Systems (UASs) achieved only 3,909 hours annually, far less than either the 7,336 flight hours that were scheduled or the 13,328 annual hours that would be needed to meet "the mission availability objective."[186] This means that, at that time, CBP's drones were flying on average less than 12 hours per week or just 29 percent of the necessary amount.[187] Similarly, a 2012 GAO audit found that the Office of Air and Marine "met 73 percent of the 38,662 air support requests and 88 percent of the 9,913 marine support requests received in fiscal year 2010," which was below OAM's goal of fulfilling more than 95 percent of Border Patrol's air support requests.[188]

Corruption Likely Undermines Border Security Operations

Adding to DHS's difficulties ensuring border security is the problem of potential corruption within the Department's workforce; which causes additional operational challenges. The issue of potential corruption within CBP is well-documented. For example, GAO issued a report on corruption and misconduct in December 2012, finding that more than 140 current and former CBP employees had been arrested for corruption offenses, such as smuggling, and 125 had been convicted as of late 2012.[189] The majority of those cases occurred near the Southwest border. The problem of corruption is further evidenced by the high number of investigations of CBP employees. In 2011, the DHS Office of Inspector General had 600 open investigations examining CBP employees.[190] In 2012, the OIG transferred 370 cases involving CBP and ICE

[184] Minority staff notes of CBP's FY2015 budget briefing before the Senate Homeland Security and Governmental Affairs Committee.
[185] Ibid.
[186] DHS Office of Inspector General, CBP's Use of Unmanned Aircraft Systems in the Nation's Border Security, OIG-12-85, May 2012, p.4.
[187] Ibid, p.4.
[188] Government Accountability Office, "Border Security: Opportunities Exist to Ensure More Effective Use of DHS's Air and Marine Assets," GAO-12-518, March 2012, Highlights.
[189] Government Accountability Office, "Border Security: Additional Actions Needed to Strengthen CBP Efforts to Mitigate Risk of Employee Corruption and Misconduct," GAO-13-59 (Washington, D.C.: Dec. 4, 2012), Highlights.
[190] Jordy Yager, "Corruption a problem at Customs and Border Protection, agency head says," The Hill, June 12, 2011.

employees to ICE's internal investigative office, due to the then-Acting Inspector General's concerns that the OIG was unable to manage the workload.[191] A review of DHS documents made available to the Committee reveals that DHS has also identified corruption within its own ranks as a problem that must be overcome.[192] Some DHS officials have also pointed to a hiring surge since 2006 as a factor contributing to the problem of corruption.[193]

Complicating the problem of apparent corruption within the CBP workforce is the inability of DHS and CBP to swiftly investigate incidents or mitigate the apparent problem. Recent reports focused on systemic failures of CBP's internal investigators, the Internal Affairs Division, whose responsibilities include investigating different aspects of misconduct at the agency.[194] Such misconduct can range from relatively minor infractions to charges of accepting bribes from drug traffickers.[195] Elements of this division are reportedly under investigation for "falsifying documents, intentionally misplacing employee complaints and bungling misconduct reports as part of a cover-up to mask its failure to curb employee wrongdoing," according to an investigation by the Washington Bureau of McClatchy.[196]

In June, James F. Tomsheck was removed from his position as the head of CBP Internal Affairs amid these questions.[197] For his part, Mr. Tomsheck offered his perspective of the problem of corruption within CBP and DHS, and spoke with Committee staff on the issue. He identified several systemic problems within CBP, including the organization's past failure to use polygraphs when screening applicants. Mr. Tomsheck also alleged that, in the past, a former CBP Commissioner and other senior Department officials communicated to him a concern about

[191]Committee minority staff review and analysis of documents provided by DHS and Customs and Border Protection and DHS.
[192]Ibid.
[193]GAO also reported that several DHS officials testified before the Senate in 2011 that the hiring of more than 8,000 employees since 2006 increased the likelihood of corruption, since it expanded opportunities for adversaries seeking to infiltrate or corrupt the CBO workforce. See: Government Accountability Office, Border Security: Additional Actions Needed to Strengthen CBP Efforts to Mitigate Risk of Employee Corruption and Misconduct, GAO-13-59, December 4, 2012, p.2. In fiscal year 2012, CBP allocated approximately $166 million for integrity programs.
[194]Marisa Taylor, "Customs under fire for sweeping scans of employees' personal data," McClatchy Washington Bureau, July 8, 2014.
[195]Marisa Taylor and Franco Ordonez, "Border Patrol watchdog under investigation for rapes, abuse, bribes from drug lords", McClatchy Washington Bureau, June 20, 2014.
[196]Ibid.
[197]Ibid.

the number of corruption investigations that CBP Internal Affairs was completing.[198] Mr. Tomsheck made some of these allegations publicly, including telling *The Washington Post* that an estimated 5 to 10 percent of Border Patrol workers engaged in corrupt activities during their careers.[199] While the veracity of Mr. Tomsheck's statements may be questioned based on the circumstances of his departure from CBP, the allegations are troubling, and suggest that the problem of corruption within CBP may be significant. This issue should be a priority for ongoing Congressional and independent oversight.

Aviation Security

Along with securing the border, DHS is charged with securing the skies. Securing air travel has been a priority for the nation since the morning of September 11, 2001. Terrorist groups, including al-Qa'ida, and its affiliates, as well as other Islamic extremist organizations, continue to plot or aspire to conduct terrorist attacks on aviation systems. There has fortunately not been a significant, successful terrorist attack on a U.S. flight since 2001, though there have been multiple "near miss" incidents where tragedy and significant loss of life were only narrowly avoided.

The Department of Homeland Security has key responsibilities for aviation security and air travel, primarily through the Transportation Security Administration (TSA). DHS faces a challenge from adversaries intent on conducting terrorist attacks against airliners.[200] Such attackers will likely continue to develop new technologies to defeat the current generation of security measures, including screening technologies that governments deploy to prevent attacks. This reality forces DHS and TSA, as well as other foreign governments, to play a cat-and-mouse game of continuously anticipating the next threat and developing screening technologies, mechanisms, and tactics to disrupt future plots.

---

[198] August 6, 2014 interview with Committee staff. In one example, Mr. Tomsheck told Committee staff that a senior CBP official wrote a number on a paper in a meeting with Mr. Tomsheck and a colleague, implying that the number of CBP Internal Affairs arrests should be lowered to that number per year. Mr. Tomsheck told staff that the implication was clear that CBP leadership wanted few corruption investigations and arrests.

[199] Andrew Becker, "Border agency's former watchdog says officials impeded his efforts," Washington Post, August 16, 2014.

[200] There have been several reported plots against commercial aviation in recent years. For example, see: Scott Shane and Eric Schmitt, "Qaeda Plot to Attack Plane Foiled, U.S. Official Say," The New York Times, May 7, 2012. An assumption of current U.S. policy related to aviation security policy is that adversaries committed to conducting terrorist attacks against the United States will likely continue to plot or aspire to plot terrorist attacks against aviation systems.

DHS has made improvements with its aviation security initiatives,[201] and recognizing the difficult challenges that DHS and TSA face, it is understandable that not all of DHS's projects will be successful. Unfortunately, however, a review of the available oversight work regarding TSA's tactical and technological programs for aviation screening reveals some concerns. There have been several instances of wasteful and ineffective TSA aviation security programs, which appear to have yielded little in the way of improved security despite significant taxpayer expenditures.

For example, since 2007, TSA has deployed Behavioral Detection Officers (BDOs) to airports to execute its Screening of Passengers by Observation Techniques (SPOT) program, which is intended to identify suspicious passengers based on their behavior at the airport. In 2013, GAO presented the results of an audit of the SPOT program and recommended that "TSA should limit future funding for behavioral detection activities," based on the lack of scientific or empirical evidence to support the use of nonverbal behavioral detection and methodological problems of DHS's SPOT validation study.[202] TSA has spent $900 million on this program since 2007, even though it appears to be doing little to make our skies safer from potential terrorist attacks.[203]

TSA's attempts to deploy effective technology screening machines for both baggage and passengers have also faced questions about efficiency and efficacy. In 2012, for example, an investigative report prepared by two House of Representative committees highlighted "serious inefficiencies in TSA's management and deployment of screening technology," including examples of thousands of machines going unused and sitting in warehouses, in some cases for periods of 6 months to even years.[204] For example, in 2011, GAO found that some of the explosive detection systems that DHS and TSA had acquired to screen checked baggage were not meeting 2005 standards for explosive detection, but instead were set to meet 1998 standards, raising questions about whether such technology investments would be successful in detecting small

[201] "Improving Aviation Security," Department of Homeland Security, at: http://www.dhs.gov/aviation-security, accessed December 31, 2014.
[202]Government Accountability Office, Aviation Security: TSA Should Limit Future Funding for Behavior Detection Activities, GAO-14-158T, November 14, 2013.
[203]Ibid., p. 2
[204]Committees on Oversight and Government Reform and Transportation and Infrastructure, "Airport Insecurity: TSA's Failure to Cost-Effectively Procure, Deploy, and Warehouse Its Screening Technologies," Joint Majority Staff Report, 112th Congress, May 9, 2012.

amounts of explosives packaged in baggage.[205] The Department and TSA have faced similar challenges deploying checkpoint explosives detection equipment such as with advanced imaging technology.[206]

In some cases, TSA's technologies have faced serious questions about safety and privacy. In 2013, TSA announced that it was removing the X-Ray scanning systems that had been deployed to airports, in response to concerns that the screening systems produced naked images of passengers and that TSA could not ensure that it was meeting privacy guidelines.[207] In all, DHS had acquired 251 of these machines at a cost of more than $41 million.[208] Others have questioned the safety of the machines, and whether TSA had satisfactorily studied any potential health risks before using the machines at airports.[209] Senator Coburn sponsored bipartisan legislation along with four members of the Committee in the 112th Congress to require DHS to commission an independent study of the use of machines,[210] and a similar requirement was ultimately included in report language for an appropriations bill. In 2012, TSA announced it was commissioning an independent study of the machines.[211] In November 2014, the National Academy of Sciences reported that the study was planned to be released by January 2015.[212]

[205]Government Accountability Office, "Homeland Security: DHS and TSA Continue to Face Challenges Developing and Acquiring Screening Technologies, Testimony Before the Subcommittee on Transportation Security, Committee on Homeland Security, House of Representatives, GAO-13-469T, May 8, 2013. GAO reports that the exact number of machines could not be reported publicly because it was sensitive security information.
[206]Government Accountability Office, Advanced Imaging Technology: TSA Needs Additional Information before Procuring Next-Generation Systems, GAO-14-357,; Government Accountability Office, Homeland Security: DHS and TSA Continue to Face Challenges Developing and Acquiring Screening Technologies, GAO-13-469T, May 8, 2013.
[207] Adam Snider, "TSA pulls plug on 'naked' body scanners." Politico, Jan. 18, 2013.
[208] DHS Office of Inspector General, "TSA's Management of Secure 1000SP Advanced Imaging Technology Units," September 2014, OIG 14-138, p.1.
[209]Michael Grabell, "U.S. Government Glossed Over Cancer Concerns As It Rolled Put Airport X-Ray Scanners," ProPublica, November 1, 2011.
[210]U.S. Senate Committee on Homeland Security and Governmental Affairs: "Senators Collins, Akaka, Levin, Coburn, Scott Brown introduce bill to require study, warnings of health effects of some airport scanners." Minority Media, Jan. 31, 2012.
[211]Michael Grabell, "U.S. Government Glossed Over Cancer Concerns As It Rolled Put Airport X-Ray Scanners," ProPublica.
[212]Minority Staff, Phone Call with Government Affairs Representative of National Academy of Sciences, November 6, 2014.

Federal Air Marshals

Another key program that TSA counts on to secure our flights is the Federal Air Marshals (FAMs) program, which deploys law enforcement officers to fly on certain flights to deter or mitigate potential threats posed by terrorists.[213] The FAMs program was expanded due to the September 11 attacks, and the need to prevent potential disruptions, including hijackings, during commercial flights. However, in part due to limited publicly available oversight evidence[214], it is unclear to what extent the FAMs program is reducing risk to aviation security, despite the more than $820 million annually that is spent on the program.[215]

Since 2001, DHS and TSA have deployed a series of new security mechanisms to mitigate the risk of certain attacks, including the type of hijacking attack executed in 2001.[216] For example, a would-be hijacker attempting a plot similar to what occurred on September 11th would likely be stopped by the various screening mechanisms before he is able to board the plane. If he defeated these screening mechanisms, he would encounter a locked cockpit door and potentially an armed pilot in the cockpit, should he attempt a hijacking. It is not clear that the FAMs program and its strategy for allocating resources, including assigning federal air marshals to certain flights, has kept pace with these changes and security enhancements. In recognition of these new security protocols that have been deployed at airports and on aircraft, FAMS has conducted a strategy and resources review and will implement new deployment matrices based on their findings. Whether and how the new strategy buys down risk at an acceptable cost remains to be determined.[217] Ensuring that the FAMs program, and its operations for domestic and international flight programs, are up-to-date and focused on areas where it can yield a significant security enhancement should remain a priority for DHS and a focus of ongoing oversight.

---

[213] "Federal Air Marshals," Department of Homeland Security, at: http://www.tsa.gov/about-tsa/federal-air-marshals , accessed December 31, 2014.
[214] There has been limited oversight done of the FAMs program and some of the work that has been done has been classified given the sensitive security information involved with the FAMs program and how resources are deployed.
[215] William L. Painter, "Department of Homeland Security: FY2014 Appropriations," Congressional Research Service, April 18, 2014.
[216] "Improving Aviation Security," Department of Homeland Security, at: http://www.dhs.gov/aviation-security, accessed December 31, 2014.
[217] Minority staff notes of FAMs' briefing before Senate Homeland Security and Governmental Affairs staff on September 13, 2014.

Ports and Sea Borders and Safeguarding Cargo Shipping

In addition to securing land borders and aviation security, DHS and its components have a primary role in securing our nation's seaports, which are a key part of the nation's and the world's supply chain infrastructure. Port security has long been recognized as a significant challenge for the nation. In the fall of 2000, for example, a national commission established by President Clinton found that security at U.S. ports was often lacking.[218] Following the 2001 terrorist attacks, securing ports became a pressing priority for the U.S. government. Through legislation and executive action, Congress and the White House constructed a comprehensive—and costly—strategy to secure U.S. ports, including background checks and special IDs for all port personnel, 100 percent radiation scanning for all cargo before it reached the United States, and massive security upgrades for port security, among other measures.

Despite spending approximately $5 billion on projects to secure port infrastructure[219], cargo containers, and port workers, the Department of Homeland Security cannot assure that our ports are secure from a potential terrorist attack.[220] For example, DHS has spent over $2.3 billion on the Port Security Grant Program (PSGP),[221] which was aimed to help states and localities harden port infrastructure, but DHS does not know how that money has improved security at our nation's ports, track with any practical accuracy how those funds are spent, or study what projects or expenditures are more effective than others in improving security.[222]

---

[218] The Report of the Interagency Commission on Crime and Security at U.S. Seaports found that the "state of security in U.S. seaports generally ranges from poor to fair, and, in some cases, good." The Commission determined that there were "no widely accepted standards or guidelines for physical, procedural, and personnel security for seaports," adding that the lack of identification cards was a problem. The Report on the Interagency Commission on Crime and Security in U.S. Seaports, Fall 2000.

[219] The Department has several programs for port security. According to information provided to the minority staff by DHS, the Department has spent approximately $5.167 billion on its various initiatives related to port security since 2002, including $2.958 billion on the Port Security Grant Program, 959 million on the Container Security Initiative, 411.9 million on the Customs-Trade Partnership Against Terrorism, 336.7 million on the Automated Targeting System, 60 million on the Secure Freight Initiative, $21.8 million on the Coast Guard's waterways and coastal security efforts, and $420 million on the Transportation Worker's Identification Credential. Committee staff analysis December 2014.

[220] "Evaluating Port Security: Progress Made and Challenges Ahead," Senate Homeland Security and Governmental Affairs Committee hearing, June 4, 2014.

[221] Federal Emergency Management Agency, National Award Summary Report Data as of May 15, 2014.

[222] In a November 2011 report, GAO recommended that DHS strengthen its methodology for measuring vulnerability in ports by accounting for how past security investments reduce vulnerability and by using the most precise data available. "Port Security Grant Program: Risk Model, Grant Management, and Effectiveness Measures Could Be Strengthened," GAO, November 2011, p. 2, http://www.gao.gov/products/GAO-12-47, accessed July 27, 2014. At a June 2014 Committee hearing, GAO reported about FEMA's response to GAO's 2011 recommendation: "In February 2014, FEMA officials stated that they have determined that this specific enhancement is not achievable, in part because the agency lacks the resources to annually measure the reduced vulnerability attributed

Moreover, as years pass and new measures are installed, DHS does not take completed projects into account when distributing PSGP funds.[223] All too often, state and local governments are using the millions in PSGP funds they receive to pay for routine expenditures, or in some cases, unnecessary equipment not directly focused on improving port security. Some examples of PSGP-grant funded expenditures that are not directly focused on improving port security include: Portland, ME's purchase of a Lenco Bearcat armored vehicle[224], Suffolk, VA's purchase of a $656,000 custom-made bus to serve as a mobile command vehicle[225], and several Connecticut towns using $28,000 in PSGP funds to purchase diving training at the Boys and Girls Club of Greenwich, CT for search and rescue operations for emergency responders.[226]

DHS was also required to secure port infrastructure and facilities by creating an identification card for transportation workers to enter secure areas, including ports. After twelve years, the Transportation Workers Identification Credential (TWIC) is incomplete and poorly managed despite receiving nearly $360 million in funding, from appropriations and user fees.[227] GAO audits have identified weaknesses in the TWIC program, including a 2013 audit that determined that the card readers that DHS was using in a pilot program were "unreliable"[228] and needed to be reassessed. At a 2014 hearing, a DHS official told Senator Coburn that "we're two and a half years or so away from the date that I anticipate card readers will be required at certain port facilities," which essentially renders TWIC cards to be a photo ID.[229] There are also questions about whether the TWIC card program used appropriate vetting procedures, including those raised by a GAO audit identifying problems with the TWIC program's internal controls for background checks[230] and the March 2014 shooting at the Naval

---

to the enhanced PSGP security measures." Statement of Stephen L. Caldwell, "Maritime Security: Progress and Challenges with Select Port Security Programs," June 4, 2014, Senate Homeland Security and Governmental Affairs Committee.

[223] Ibid.

[224] Dennis Hoey, "Portland Police add armored vehicle to its force," Portland Press Herald, June 7, 2012.

[225] Jeff Sheler, "Suffolk mobile command center revved for action," The Virginian-Pilot, September 30, 2012.

[226] Barbara Heins, "Diving for Experience: Emergency responders from Greenwich, Stamford, Westport, Milford participate in regional dive training operations," Stamford Patch, March 13, 2014.

[227] Minority staff analysis of spending data provided by DHS. The TWIC program has received approximately $111.4 million in appropriations and more than $247 million from user fees.

[228] GAO, "Transportation Worker Identification Credential: Card Reader Pilot Results are Unreliable; Security Benefits Need to Be Reassessed," May 2013, GAO-13-198.

[229] Comments of Real Admiral Paul F. Thomas, U.S. Coast Guard, in response to Dr. Coburn's questions. Senate Homeland Security Committee Hearing, June 4, 2014.

[230] Statement of Stephen L. Caldwell, "Maritime Security: Progress and Challenges with Select Port Security Programs," June 4, 2014, Senate Homeland Security and Governmental Affairs Committee.

Station in Norfolk, conducted by a truck driver who used his TWIC card to gain access to the facility despite a prior criminal record.[231]

DHS also has responsibilities for safeguarding lawful trade. For the purposes of addressing security risks to the homeland, the most significant challenge for safeguarding trade that DHS has faced is the screening of cargo to ensure that potential weapons of mass destruction, such as nuclear devices, do not enter U.S. ports. In 2007, President Bush signed the Implementing Recommendations of the 9/11 Commission Act of 2007, which required 100 percent of all containers loaded on a vessel in a foreign port be scanned by nonintrusive imaging and radiation equipment before entering the United States.[232]

Despite spending $2.1 billion on Customs and Border Protection's cargo screening program, the 100 percent radiation screening mandate established by the 2007 law still has not been met and DHS officials have reported that it will never be achieved. [233] Both Congress and DHS leadership have failed to develop a clear and consistent strategy for meeting this mandate. In fact, both have funded and directed CBP programs that promote opposing results. Former Secretary Janet Napolitano said in a 2012 hearing before the House Homeland Security Committee "the mandate isn't practicable or affordable."[234]

CBP has also struggled with the management of a large and complex information technology acquisition and development project to streamline information processing for cargo shipping. In 2001, the federal government launched the Automated Commercial Environment (ACE), an initiative to create a system for electronically submitting and tracking information about import and export goods, which was originally projected to take 5 years to build at a cost of $1.3 billion dollars.[235] Repeated oversight audits have tracked DHS's struggle to manage the program over the past decade, including the lack of realistic goals in the program.[236] In 2014, the

[231] Mark Rockwell, "Does TWIC really work?," Federal Computer Week, June 5, 2014.
[232] P.L. 110–53—AUG. 3, 2007.
[233] Opening Statement of Senator Tom Coburn, "Evaluating Port Security: Progress Made and Challenges Ahead," Senate Homeland Security and Governmental Affairs Committee, June 4, 2014.
[234] Bliss, Jeff, "U.S. Backs Off All-Cargo Scanning Goal With Inspections at 4%," Bloomberg, August 13, 2012. http://www.bloomberg.com/news/2012-08-13/u-s-backs-off-all-cargo-scanning-goal-with-inspections-at-4-.html, accessed August 15, 2013.
[235] Elizabeth Newell Jochum, "GAO sees progress, ongoing problems in DHS cargo program," Government Executive, October 26, 2007.
[236] Daniel Pulliam, "DHS trade processing system lacks realistic goals, GAO says," Government Executive, June 2, 2006.

ACE program's lifecycle cost estimate had increased to $4.5 billion.[237] But CBP reports that ACE's program completion remains years away. According to a December 2013 briefing, CBP's goal for the program was to "develop all core trade processing capabilities in ACE in approximately three years."[238] If this goal is met, DHS will have completed its revamp of the cargo shipping information processing system 15 years after the initiative began.

Disrupting and Dismantling Transnational Criminal Organizations

As part of DHS's second mission of securing and managing our nation's borders, the Department's strategy lists an additional objective: disrupting and dismantling transnational criminal organizations. Key DHS components, including the Coast Guard, Immigration and Customs Enforcement, and the Secret Service, have significant responsibilities for interdicting or investigating and arresting criminals or threats, including transnational criminal organizations. However, this objective appears to be merely an aspirational goal for the Department. It is unlikely to be accomplished, or even to be a significant area of DHS's work, because it is not the sole or primary focus of any of the involved components.

Coast Guard, Immigration and Customs Enforcement and the U.S. Secret Service all have responsibilities for investigating or disrupting international criminal activity; however, each of these components have other competing, and in fact higher-priority, responsibilities within their own missions. As will be discussed in the following section, Immigration and Customs Enforcement has a lead responsibility within the Department for investigating and arresting members of transnational criminal organizations; however, ICE has several competing responsibilities, and its resources for stopping international crime are dwarfed by other federal agencies, including the Federal Bureau of Investigation and the Drug Enforcement Agency. Similarly, the U.S. Secret Service, which investigates international financial crimes and enforces other laws, has more pressing responsibilities related to its protection and security missions, as was discussed in the previous section. For both agencies, some of their investigative and law enforcement responsibilities are duplicative or overlap the jurisdictions and work of other

[237] This cost estimate was provided by the Inspector General. Statement of John Roth, Inspector General, Department of Homeland Security, Committee on Homeland Security, U.S. House of Representatives, May 7, 2014.
[238] U.S. Customs and Border Protection, "Automated Commercial Environment Update," PowerPoint Presentation, December 2013, at: http://www.cbp.gov/sites/default/files/documents/ace_ovrview_status_4.pdf, accessed November 5, 2014.

significant and experienced federal law enforcement organizations. The Coast Guard, for its part, has eleven diverse and competing missions[239], as is discussed later in this report, prohibiting it from focusing on its missions of drug interdiction and disrupting criminal activity.

Each of these components can point to successes and results from their respective law enforcement missions, and each contributes to the mission of disrupting transnational criminal organizations. For example, the USSS reported making nearly 2,700 counterfeiting arrests worldwide in 2013, recovering $156 million in counterfeit U.S. currency. The Secret Service also made 35 international arrests for money laundering and identified more than $831 million in its financial crimes investigations. [240] One successful investigation that the USSS described in its annual report was an investigation that resulted in the arrest of 10 criminals who fraudulently withdrew $2.8 million from ATMs in New York. [241] ICE's Homeland Security Investigations does not prepare an annual summary of the results of its investigations, as was requested by staff; therefore, a topline summary of ICE's investigations is not available to report.[242] However, ICE too has demonstrated some successes in disrupting international criminal organizations. For example, Secretary Jeh Johnson announced in July 2014 that ICE arrested and dismantled a human smuggling operation in South Texas, including arresting 192 smugglers.[243] Coast Guard can also point to significant successes enforcing federal laws and stopping criminal activity. For example, the Coast Guard reports stopping 125 metrics tons of illegal drugs, which was estimated to be worth $3 billion, and detained more than 190 smugglers in 2013.[244] These successes aside, disrupting transnational criminal organizations is not the primary mission of ICE, Secret Service, or Coast Guard, which raises the question of whether this objective of DHS's second strategy is realistic or simply aspirational.

Conclusion

Securing and managing the nation's border is the second mission of the Department, and DHS allocates significant resources to accomplish this strategy objective. Unfortunately,

[239] U.S. Coast Guard, "Missions," at: http://www.uscg.mil/top/missions/, accessed December 23, 2014.
[240] U.S. Secret Service Annual Report, 2013, at http://www.secretservice.gov/USSS_FY13AR.pdf, accessed December 29, 2014.
[241] Ibid.
[242] ICE Office of Congressional Relation's email to HSGAC minority staff, October 30, 2014.
[243] "Secretary Jeh Johnson Announces 192 Criminal Arrests in Ongoing ICE Operation to Crack Down on Human Smuggling to the Rio Grande Valley," DHS Press Office, July 22, 2014.
[244] United States Coast Guard, 2015 Budget in Brief – 2013 Performance Highlights.

evidence shows that the Department has not yet succeeded. A review of CBP's strategies and corridor campaign plans for the Southern and Northern Borders reveal vast expanses where few assets are deployed to prevent illegal entry, and DHS's struggle to deploy other assets, such as aerial surveillance, suggests that these gaps are likely being exploited. In order to secure the southern and northern border, DHS must overcome several challenges, including developing a department-wide plan or strategy that aligns components' activities, a step that the Department has taken thanks to Secretary Johnson's leadership. But DHS and CBP must also improve resource allocation and operations, as well as resolve the problem of potential corruption within CBP's workforce, a key vulnerability that must be eliminated to secure the border. In the area of aviation security, DHS has made significant improvements. But the available oversight work that has been done raises questions about the efficiency and effectiveness of some of TSA's efforts to mitigate the serious threat of terrorist plots against commercial aviation, suggesting that there is an opportunity for improvement. Similarly, the Department, including CBP and FEMA, have devoted considerable resources to securing U.S. ports and improving processes to scan and track cargo moving in and out of the United States, but many of the basic objectives that the Department and Congress set to secure our ports and supply chain have not been accomplished. And while the Department—including ICE, Secret Service and Coast Guard—works to accomplish the Department's objective of disrupting transnational criminal organizations, this is not any component's primary responsibility, raising the question of whether the Department is well-suited to succeed in this area.

Mission 3— Enforcing and Administering Our Immigration Laws

Overview

The Department of Homeland Security's third mission is to enforce and administer our nation's immigration laws. Prior to 2002, Immigration and Naturalization Services (INS) managed these responsibilities under the leadership of the Department of Justice. The Homeland Security Act of 2002 eliminated INS and separated it into three new components of the Department of Homeland Security: U.S. Citizenship and Immigration Services (USCIS), Immigration and Customs Enforcement (ICE), and Customs and Border Protection (CBP).[245]

After nearly 13 years, the Department of Homeland Security components responsible for administering and enforcing the nation's immigration laws continue to struggle with this mission. A review of the available information about USCIS and ICE's performance related to immigration administration and enforcement raises serious questions about whether the current structure of DHS's components and programs for immigration administration and enforcement is well-suited to accomplishing the Department's third mission.

U.S. Citizenship and Immigration Services has faced challenges with its basic responsibilities of efficiently managing the administration system. For example, USCIS has struggled with delays and cost overruns of its various information technology transformation projects; which were intended to improve both customer service and federal oversight of the immigration system. [246] USCIS has also historically struggled to process immigration petitions and caseloads in a timely manner.[247] Questions remain about whether the agency has succeeded in its more than a decade-long effort to erase the immigration benefits processing backlog and carry out timely processing. Given these ongoing challenges, Congress and the Department should question whether USCIS is well-equipped to process new work visas and other

[245] "Overview of INS History," USCIS History Office and Library, U.S. Citizenship and Immigration Services, 2012, at 9, at http://www.uscis.gov/sites/default/files/USCIS/History%20and%20Genealogy/Our%20History/INS%20History/INSHistory.pdf, accessed December 29, 2014; see also Ruth Ellen Wasem, "Toward More Effective Immigration Policies: Selected Organizational Issues," Congressional Research Service, RL33319, January 25, 2007, p. 3.
[246] DHS Office of Inspector General, "U.S. Citizenship and Immigration Services' Progress in Transformation," OIG-12-12, November 2011; Aliya Sternstein, "After Delays, USCIS Sets New Deadline for Digital Immigration Records," NextGov.com, July 29, 2014.
[247] William A. Kandel, "U.S. Citizenship and Immigration Services' Immigration Fees and Adjudication Costs: Proposed Adjustments and Historical Context," Congressional Research Service, RL34040, July 16, 2010, p.24.

temporary immigration benefits for those eligible under President Obama's November 2014 executive action.[248] Beyond these issues with the basic tasks of efficiently administering immigration benefits, USCIS has faced questions about its ability to prevent fraud and mitigate national security concerns.

DHS and its Immigration and Customs Enforcement (ICE) component has also struggled to achieve its primary mission of effectively enforcing the nation's immigration laws. According to the most recent data available from DHS, there were approximately 11.4 million unauthorized immigrants living in the United States as of 2012.[249] ICE reported conducting 315,943 removals in FY 2014.[250] The current focus of ICE's Enforcement and Removal Operations has been on removing criminal aliens and apprehending and removing illegal immigrants who were caught near the border, meaning that the agency does little immigration enforcement within the nation's interior.[251] According to an analysis by experts writing for the Council on Foreign Relations in 2013, the chance of an illegal immigrant being removed by DHS is approximately 3.26 percent.[252] This suggests that DHS is not doing enough to enforce immigration laws, including tracking and removing the millions of people who have legally entered the United States and then overstayed their visa. Though DHS claims to focus on removing criminal aliens, the Inspector General found that ICE released more than 2,000 illegal immigrant detainees in February 2013, including more than 600 aliens with criminal records; creating a risk to public safety and undermining the Department's credibility as an agency that enforces the rule of law.[253]

The Department's components responsible for immigration oversee programs that have significant vulnerabilities that potentially undermine national security. Immigration and

---

[248] Executive Actions on Immigration, U.S. Citizenship and Immigration Services, at: http://www.uscis.gov/immigrationaction, December 31, 2014.
[249] Bryan Baker and Nancy Rytina, "Estimates of the Unauthorized Immigrant Population Residing in the United States: January 2012," U.S. Department of Homeland Security, Office of Immigration Statistics, 2014, at: http://www.dhs.gov/publication/estimates-unauthorized-immigrant-population-residing-united-states-january-2012, accessed December 23, 2014.
[250] Department of Homeland Security, "DHS Release End of the Year Statistics," December 19, 2014.
[251] ICE reported that for FY2014, 213,719 of the 315,943 removals it conducted that year were "apprehended while, or shortly after, attempting to illegally enter the United States. ICE removed 102,224 people who were apprehended within the U.S. interior, and of these, 85 percent were previously convicted of a criminal offense. Department of Homeland Security, "DHS Release End of the Year Statistics," December 19, 2014.
[252] Council on Foreign Relations, "Managing Illegal Immigration to the United States: How Effective Is Enforcement?," May 2013, p. 29.
[253] "ICE's Release of Immigration Detainees," Department of Homeland Security Office of Inspector General, OIG-14-116, August 2014.

Customs Enforcement is responsible for administering the Student Exchange and Visitor Program (SEVP), which is allowing 1.3 million students and visitors to stay in the United States in order to study or work.[254] However, several watchdog audits show that ICE is not effectively managing this program or ensuring that SEVP participants are meeting the terms of their visa.[255] Poor management of the student and visitor visa programs invites a potential risk to national security. In the past, people plotting terrorist attacks, including several of the 9/11 hijackers, were in the United States on student visas[256].

USCIS also manages a program which invites fraud and creates national security vulnerabilities. The Employment-Based 5th Preference (EB-5) visa program allows immigrants to gain entry into the United States if they make investments totaling $500,000 or $1,000,000 in business enterprises that create economic activity and jobs within the United States. This includes investing in USCIS-approved "Regional Centers," which pool funds and make investments. Participation in the EB-5 visa program has increased significantly under the current administration, from 1,360 immigrant investors in 2008 to 6,628 as of 2012.[257] Several reviews of this program, including an independent audit and an internal review apparently ordered by the White House[258], reveal significant vulnerabilities in this EB-5 visa program, including its vulnerability to exploitation by criminals, terrorists, foreign government agencies and intelligence operatives, as well as other adversaries.[259] For example, a December 2013 Inspector General audit of DHS's management of the EB-5 program found that "USCIS is limited in its ability to prevent fraud or national security threats that could harm the United States."[260]

---

[254] U.S. Immigration and Customs Enforcement, Student Exchange Visitor Program, "SEVIS by the Numbers: General Summary Quarterly Review, October 2014.
[255] Government Accountability Office, Student and Exchange Visitor Program: DHS Needs to Assess Risks and Strengthen Oversight Functions, June 2012.
[256] Minority committee staff interview with ICE HSI Special Agent Brian Smeltzer, Unit Chief, Counterterrorism and Criminal Exploitation Unit, July 1, 2014.
[257] "EB-5 Immigrant Investor Frequently Asked Questions," USCIS, at: http://www.uscis.gov/working-united-states/permanent-workers/employment-based-immigration-fifth-preference-eb-5/eb-5-immigrant-investor, accessed November 6, 2014.
[258] Forensic Assessment of Financial Flows Related to EB-5 Regional Center, Document Marked Draft and Pre-Decisional, National Security Staff.
[259] Undated Memorandum, U.S. Customs and Immigration Enforcement on Implications of U.S. Immigration and Customs Case Against Procurement Agent. U.S. Immigration and Customs Enforcement, Homeland Security Investigations, "EB-5 Program Questions from DHS Secretary." Senator Grassley published a redacted copy of the document on his website, at: http://www.grassley.senate.gov/sites/default/files/issues/upload/EB-5-12-12-13-ICE-memo-security-vulnerabilities.pdf (Accessed: December 28, 2014).
[260] Department of Homeland Security, Office of the Inspector General, "United States Citizenship and Immigration Services' Employment-Based Fifth Preference (EB-5) Regional Center Program," OIG-14-19, December 2013, p.5.

Oversight of the program, including surveying 430 regional centers participating in the program, raised additional questions about the EB-5 visa program, and about why the Department continues to operate and expand a program that is known to be vulnerable to criminal and national security threats.

Given these struggles, Congress and the Department of Homeland Security should review and reconsider its current approach to administering and enforcing immigration laws. For example, Congress should consider whether resources within the Department's budget could be refocused and reprioritized to the immigration law enforcement mission to ensure that the rule of law is upheld. For example, ICE's significant resources devoted to non-immigration enforcement investigations, including intellectual property violations within the nation's interior, should be reviewed and reprioritized. Congress should also reconsider whether it was prudent to sever the joint missions of INS for immigration benefits administration and immigration law enforcement into two separate components. Congress should also end, suspend, or fundamentally reform the immigration benefits programs managed by DHS that create potential vulnerabilities for national security, including the SEVP and EB-5 visa programs.

U.S. Citizenship and Immigration Services (USCIS): Administering the Immigration System

According to its website, USCIS, which officially assumed the immigration service responsibilities of the federal government on March 1, 2003,[261] exists "to enhance the security and efficiency of national immigration services by focusing exclusively on the administration of benefit applications."[262] It is the only one of the three immigration-related DHS components that has only immigration-related responsibilities.[263] USCIS currently has 19,000 government employees and contractors at 223 offices throughout the world.[264] USCIS has three major functions—adjudication of immigration petitions, adjudication of naturalization petitions and

[261] Website of U.S. Citizenship and Immigration Services, About, Our History, at http://www.uscis.gov/about-us/our-history, accessed April 9, 2014.
[262] Ibid.
[263] Wasem, Ruth Ellen, "Toward More Effective Immigration Policies: Selected Organizational Issues," Congressional Research Service, RL33319, January 25, 2007, p. 27.
[264] Website of U.S. Citizenship and Immigration Services, About Us, accessed April 9, 2014, available at http://www.uscis.gov/aboutus.

the consideration of refugee and asylum claims; as well as related humanitarian and international concerns.[265]

For FY 2014, USCIS's budget was $3.4 billion, approximately 5 percent of the Department's entire budget.[266] USCIS has two primary sources of funding—fee-based mandatory appropriations and discretionary appropriations.[267] The vast majority of USCIS funding comes from the fees collected for immigration services, such as applications and petitions.[268] A primary responsibility for USCIS is to swiftly process and adjudicate petitions for immigrant benefits. The number of pending cases and backlog related to processing benefits has been a challenge of USCIS and its predecessor agency INS.[269] In 2002, USCIS released a plan that would eliminate the backlog by the end of FY 2006.[270] However, the status of USCIS's immigration benefits backlog is unclear. In 2010, the Congressional Research Service reported: "Although USCIS reports that the backlog has been reduced since Congress began appropriating direct funds for backlog elimination, questions remain because of new definitions of what constitutes a backlog."[271] Some evidence suggests that it remains a problem, including a class action lawsuit that was filed in July 2014 on behalf of more than 40,000 immigrants who claim that they have faced unnecessary delays with some waiting more than two years for their

[265] Ruth Ellen Wasem, "Toward More Effective Immigration Policies: Selected Organizational Issues," Congressional Research Service; Ruth Ellen Wasem, Alison Siskin, and March Rosenblum, "DHS Immigration Functions and Implications for Comprehensive Immigration Reform," Congressional Research Service, Slideshow, March 18, 2013, at 8.
[266] DHS Office of Inspector General, "U.S. Citizenship and Immigration Services Information Technology Management Progress and Challenges," OIG-14-112, July 2014, p.3.
[267] The fee-based mandatory appropriation is comprised of the Immigration Examination Fee Account (IEFA) and two other, smaller fee sources, the H-1B Nonimmigrant Petitioner Account and the Fraud Prevention and Detection Account. William A. Kandel, "USCIS Budget Authority, Detailed: FY 2002 – FY 2015, Requested and Actual Amounts," Congressional Research Service, Excel spreadsheet prepared by Request from Senator Coburn's staff, April 14, 2014.
[268] William A. Kandel, "U.S. Citizenship and Immigration Services' Immigration Fees and Adjudication Costs: Proposed Adjustments and Historical Context," Congressional Research Service, RL34040, July 16, 2010, p.5. The fee-based mandatory appropriation has ranged from $1.45 billion to $3.37 billion per year since FY 2003. William A. Kandel, "USCIS Budget Authority, Detailed: FY 2002 – FY 2015, Requested and Actual Amounts," Congressional Research Service, Excel spreadsheet prepared by Request from Senator Coburn's staff, April 14, 2014.
[269] In November 2005, GAO reported "recurring backlogs of benefit applications have been a long-standing problem for the former Immigration and Naturalization Service (INS) whose benefit adjudication functions are now the responsibility of USCIS." Government Accountability Office, "Immigration Benefits: Improvements Needed to Address Backlogs and Ensure Quality of Adjudications," November 2005, GAO-06-20, p.2.
[270] Id, p.3.
[271] William A. Kandel, "U.S. Citizenship and Immigration Services' Immigration Fees and Adjudication Costs: Proposed Adjustments and Historical Context," Congressional Research Service, RL34040, July 16, 2010, p.24.

asylum claims to be heard.[272] Whether USCIS has succeeded in eliminating the backlog and improved processing times is a question that deserves additional oversight and review. Congress must ask whether additional fee increases are warranted to give USCIS the resources it needs to execute its responsibility for administering immigration benefits effectively.

One of the ways that USCIS could improve the efficiency of its management of administration benefits would be to improve its technology and processing systems. However, USCIS has a history of challenges and struggles is its effort to transform its information technology system, including a decade-long IT transformation project, which aims to transition USCIS from a paper-based to an electronic system for tracking and processing benefits. [273] Using a paper-based system reduces the agency's ability to manage and process the approximately 30,000 applications for benefits it receives each day and creates a cost of $314 million annually, according to the Inspector General, for shipping, storing and handling all of the paper files.[274]

In 2007, DHS launched its program to transition to an electronic system for immigration benefits applications and processing by 2013. To date, USCIS has spent more than $1 billion on the transformation initiative, according to publicly reported estimates.[275] In 2011, the Inspector General audited the Transformation Initiative and found that a series of problems, including "changes in deployment strategy and insufficiently defined system requirements" as well as "governance and staffing problems," led to delays and USCIS's continued reliance on a paper-based system.[276] To date, the project is not yet complete. In 2014, the USCIS Director announced that the new goal for completing the transformation project was the FY 2018 or 2019, at least eleven years after its original launch.[277]

---

[272] John Marzulli, "Asylum-seeking immigrants file class-action suit against federal government over interview backlog," New York Daily News, July 4, 2014.
[273] Aliya Sternstein, "DHS Takes a Second Stab at Automating Immigration Casework," NextGov.com, March 28, 2014.
[274] DHS Office of Inspector General, "U.S. Citizenship and Immigration Services' Progress in Transformation," OIG-12-12, November 2011.
[275] Aliya Sternstein, "DHS Takes a Second Stab at Automating Immigration Casework," NextGov.com, March 28, 2014.
[276] DHS Office of Inspector General, "U.S. Citizenship and Immigration Services' Progress in Transformation," OIG-12-12, November 2011.
[277] Aliya Sternstein, "After Delays, USCIS Sets New Deadline for Digital Immigration Records," NextGov.com, July 29, 2014.

Fraud and National Security Concerns in Immigration Administration

Identifying fraud and potential national security concerns among the pool of people seeking immigration benefits has historically been a challenge for DHS and USCIS. For example, in 2008, the DHS Inspector General reported that the Office of Fraud Detection and National Security (FDNS) "had limited measurable effect on benefit fraud" and that "the current USCIS strategy for addressing immigration benefit fraud yields little measurable return."[278] In a June 2013 report, the DHS IG examined the procedures used to track and monitor the petitions and applications for family-based immigration benefits suspected of fraud. The IG found:

> …fraud-related data were not always recorded and updated in appropriate electronic databases to ensure their accuracy, completeness, and reliability. Specifically, FDNS personnel did not record in appropriate electronic databases all petitions and applications denied, revoked, or rescinded because of fraud. Supervisors also did not review the data entered into the databases to monitor case resolution. Without accurate data and adequate supervisory review, USCIS may have limited its ability to track, monitor, and identify inadmissible aliens, and to detect and deter immigration benefit fraud.[279]

USCIS is required to upload fraud-related data to TECS, formerly the Treasury Enforcement Communications System. But the Inspector General found over the 4-year period from FY 2008 – FY 2011, USCIS failed to record almost half of the 1,144 findings of fraud in I-130 and I-485 forms.[280] Overall, the Inspector General concluded that USCIS struggles to detect fraud could have "increased the risk that aliens committing fraud were granted immigration benefits or given additional opportunities to apply for benefits."[281]

One challenge facing USCIS in its efforts to prevent fraud and national security risks from gaining entry or immigration status within the country is the lack of an enforcement arm within the component, since these responsibilities shifted to Immigration and Customs Enforcement when INS was disbanded. For example, the Congressional Research Service noted

[278] Department of Homeland Security, Office of the Inspector General, "Review of the USCIS Benefit Fraud Referral Process," OIG-08-09, April 2008, p.6.
[279] Department of Homeland Security, Office of the Inspector General, "U.S. Citizenship and Immigration Services' Tracking and Monitoring of Potentially Fraudulent Petitions and Applications for Family-Based Immigration Benefits," OIG-13-97, June 2013, p.3.
[280] Id. p.4.
[281] Id. pp.4-5.

that, "there is a reported lack of coordination between USCIS and ICE in the area of fraud and national security investigations."[282]

Visa Overstays and Tracking Identities of Entries and Exits

One challenge for the Department of Homeland Security that straddles both the immigration system administration and law enforcement mission is tracking and addressing the problem of people overstaying their visas, which accounts for as much as 40 percent of the illegal immigration population.[283] In 2013, GAO reported that DHS has faced challenges addressing the problem of visa overstays, including processing a backlog of more than one million records of people who had overstayed their visas.[284] GAO further pointed out that DHS had not met its requirement under federal law to regularly report estimates of the population of visa overstays.[285]

Part of the responsibility for tracking visa overstays within the Department lies with the Office of Biometric Identity Management within the DHS's National Protection Programs Directorate (NPPD),[286] the directorate which oversees many of DHS's programs related to infrastructure protection. This office was formerly known as US-VISIT. Effectively managing data related to visa overstays has been a longstanding challenge for the Department. In 2012, the DHS Inspector General reviewed the data within DHS's database for tracking biometric information, for example, finding that within the Automatic Biometric Identification System (IDENT) there were "825,000 instances where the same fingerprints were associated with

[282] Ruth Ellen Wasem, "Toward More Effective Immigration Policies: Selected Organizational Issues," Congressional Research Service, L33319, January 25, 2007, p.26.
[283] Bryan Roberts, Edward Alden, and John Whitley, Managing Illegal Immigration to the United States, Council on Foreign Relations, May 2013, p.32.
[284] Statement of Rebecca Gambler, Government Accountability Office, "Preliminary Observations on DHS's Overstay Enforcement Efforts," Testimony Before the Subcommittee on Border and Maritime Security, Committee on Homeland Security, House of Representatives, May 21, 2013.
[285] Ibid.
[286] For background on the Office's responsibilities related to overstay enforcement, see this GAO report. GAO, "Overstay Enforcement: Additional Actions Needed to Assess DHS's Data and Improve Planning for a Biometric Air Exit Program," July 2013. According to GAO, "[T]he Office of Biometric Identity Management (OBIM), within DHS's National Protection and Programs Directorate, manages the Arrival and Departure Information System (ADIS), which tracks and matches arrival and departure records for the purpose of identifying potential overstays, and the Automated Biometric Identification System (IDENT), which maintains biometric information that DHS collects from nonimmigrants upon their entry into the United States."

different biographic data."[287] Inconsistencies and problems with these data sets, the Inspector General warned, could hinder DHS's "ability to share information that could help border enforcement agencies prevent improper entries into the United States." [288]

Federal law has required the implementation of an automated biometric entry and exit system since 1996,[289] a responsibility inherited by DHS when it was formed. Implementing such a system, including biometric data that could substantiate the information provided, presents a practical challenge for the government due to the volume of people entering into the country, evidence suggests that DHS has not made much progress. In 2013, GAO reported that "DHS's planning efforts are focused on developing a biometric exit system for airports, with the potential for a similar solution at sea ports," which also suggests that no plans were underway for tracking those exiting at land ports of entry.[290] A follow-up analysis by GAO in July 2013 reported that DHS's "goal is to develop information and report to Congress about the benefits and costs of a biometric air exit options before the fiscal year 2016 budget cycle,"[291] which would mark the passing of the twentieth anniversary of Congress's original mandate for an automated entry-exit system with apparently little progress toward achieving this goal. Given its ongoing struggle to track, report statistics about, and create an entry-exit system to monitor those overstaying their visas, Congress and the Department should consider whether the Office of Biometric Identity Management, or its responsibilities, would be better housed within either USCIS or ICE, rather than in NPPD, which largely focuses on responsibilities related to cybersecurity and critical infrastructure protection.

Immigration and Customs Enforcement: Enforcing Immigration Laws

The burden of the second half of DHS's third mission—enforcing immigration laws—is largely assigned to Immigration and Customs Enforcement, another component born out of the Homeland Security Act of 2002. ICE divides its resources into two elements: Enforcement and

[287] DHS Office of Inspector General, "US-VISIT Faces Challenges in Identifying and Reporting Multiple Biographic Identities (Redacted)", OIG-12-111, August 2012.
[288] Ibid.
[289] Lisa Seghetti and Stephen Vina, "U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) Program," Congressional Research Service, January 26, 2006.
[290] Statement of Rebecca Gambler, Government Accountability Office, "Preliminary Observations on DHS's Overstay Enforcement Efforts," Testimony Before the Subcommittee on Border and Maritime Security, Committee on Homeland Security, House of Representatives, May 21, 2013.
[291] Government Accountability Office, "Overstay Enforcement: Additional Actions Needed to Assess DHS's Data and Improve Planning for a Biometric Air Exit Program," GAO-13-683, July 2013.

Removal Operations (ERO) and Homeland Security Investigations (HSI). The 2014 budget for HSI is close to $1.9 billion compared to ERO's budget of close to 2.7 billion.[292] This agency employs nearly 20,000 employees and operates 41 international field offices.[293] Despite its primary mission of immigration law enforcement, ICE has a broad investigative mission well beyond immigration law enforcement, including cultural and antiquities crimes, cybercrime, documents and benefit fraud, narcotics, foreign corruption, human trafficking, mass-marketing fraud, child exploitation, and intellectual property crimes.[294]

The Immigration Enforcement Mission

The available evidence, including the presence of an estimated more than 11 million illegal immigrants residing in the country[295], shows that DHS and ICE have failed at the basic mission of enforcing immigration laws. Indicators of ICE's struggle include its low-deportation and removal numbers, its inability to significantly affect the population of millions of people who have overstayed their visas, and its decisions to release illegal aliens with criminal records, creating a threat to public safety.

ICE's current approach to immigration enforcement is lax, with the agency applying broad prosecutorial discretion, and largely focusing on a narrow population of illegal immigrants as targets for potential removal and enforcement. John Sandweg, former Acting Director of ICE, told the Los Angeles Times, "If you are a run-of-the-mill immigrant here illegally, your odds of getting deported are close to zero—it's just highly unlikely to happen."[296] In April 2014, The Los Angeles Times reported that "expulsions of people who are settled and working in the United States" have declined by more than 40 percent since 2009.[297] In

[292] Department of Homeland Security, Immigrations and Customs Enforcement, Congressional Budget Request 2013. Volume 1.
[293] Immigration and Customs Enforcement Homeland Security Investigations, at http://www.ice.gov/contact/hsi-international-ops, accessed December 29, 2014.
[294] According to ICE Homeland Security Investigations: "HSI has broad legal authority to enforce a diverse array of federal statutes. It uses this authority to investigate all types of cross-border criminal activity, including: Financial crimes, money laundering and bulk cash smuggling; Commercial fraud and intellectual property theft; Cybercrimes ; Human rights violations; Human smuggling and trafficking; Immigration, document and benefit fraud; Narcotics and weapons smuggling/trafficking; Transnational gang activity; Export enforcement; and, International art and antiquity theft." For background on ICE and Homeland Security Investigations, see http://www.ice.gov/hsi, accessed December 28, 2014.
[295] Michael Hoefer, Nancy Rytina, and Bryan Baker, "Estimates of the Unauthorized Immigrant Population Residing in the United States: January 2011," Department of Homeland Security, Office of Immigration Statistics.
[296] Brian Bennett, "High deportation figures are misleading," Los Angeles Times, April 1, 2014.
[297] Ibid.

September, the Associated Press reported that ICE's pace for removals was 20 percent below the rate of removals in 2013, and on target to result in the lowest number of deportations since 2007.[298]

The evidence also suggests that ICE has failed to uphold its responsibility for enforcing immigration laws related to visa overstays to ensure that people, including potential threats to public safety or national security, do not violate the terms of their stay. As discussed above, visa overstays account for millions of the estimated 11 million illegal immigrants in our country. The Council on Foreign Relations reports those who overstay their visas make up approximately 40 percent of the illegal immigrant population.[299] However, GAO reported in 2013 that DHS, and therefore ICE, struggles to even provide an estimate of the overstay population, and that 266 "illegal overstays of concern" were missing as of March 2013.[300]

Over recent years, ICE prioritized the focus of its enforcement and removal investigations to criminal aliens.[301] However, even within the narrower universe of illegal aliens who are more likely to pose a threat to public safety and, therefore, are more likely to face removal or deportation proceedings, evidence suggests that ICE is shifting to a lax approach. For example, in late November 2014, the Department announced it was canceling the Secure Communities program, which was its program for identifying criminal illegal aliens across the nation.[302] Between 2009 and 2012, DHS spent roughly $750 million standing up the Secure Communities program to create a system for sharing information between DHS, FBI, and state and local law enforcement to identify and track criminal aliens.[303] According to GAO, between 2009 and 2011, the percentage of ICE's removals that were attributed to use of the Secure

[298] Alicia Caldwell, "US sharply cutting deportations," Associated Press, September 11, 2014.
[299] Bryan Roberts, Edward Alden, and John Whitley, Managing Illegal Immigration to the United States, Council on Foreign Relations, May 2013, at 32.
[300] Government Accountability Office, "Overstay Enforcement: Additional Actions Needed to Assess DHS's Data and Improve Planning for a Biometric Air Exit Program," GAO-13-683, July 2013, p.14.
[301] For example, see the Morton Memo: "Immigration and Customs Enforcement: Exercising Prosecutorial Discretion Consistent with the Civil Immigration Enforcement Priorities of the Agency for the Apprehension, Detention, and Removal of Aliens," June 17, 2011, available at: http://www.ice.gov/doclib/secure-communities/pdf/prosecutorial-discretion-memo.pdf, accessed December 29, 2014.
[302] Secretary Jeh Johnson, Memorandum for Thomas S. Winkowski, Megan Mack, Phil McNamara, "Subject: Secure Communities," November 20, 2014. Secretary Johnson wrote: 'The Secure Communities program, as we know it, will be discontinued."
[303] Office of Inspector General, "Operations of United States Immigration and Customs Enforcement's Secure Communities," OIG-12-64 , April 2012 (Revised).

Communities program grew from 4 percent to 20 percent.[304] Whatever system or policy that replaces Secure Communities to track or remove criminal illegal aliens should be an oversight priority for Congress and other watchdogs moving forward.

Another alarming example of DHS's lax approach to immigration law enforcement occurred in February 2013, when ICE released 2,226 aliens who were detained in ICE facilities pending removal proceedings.[305] Some questioned whether the decision was related to the looming sequester budget cuts. Senator Tom Coburn and Sen. John McCain requested the Inspector General review the incident and decision-making that led to the release. The Inspector General found that included among the thousands of illegal immigrant detainees released were more than 600 illegal immigrants that had prior criminal convictions.[306] The Inspector General also raised questions about the process that led to the release, including ICE's executive leadership's failure to effectively communicate with the DHS Secretary and the White House about its fiscal challenges or plan to release the detainees.[307] ICE did not even notify the DHS Secretary about the plan or potential consequences of releasing 1,450 detainees over one weekend.[308] The Inspector General further warned that ICE still has not developed a strategy to effectively manage its detention program.[309]

In October 2014, USA Today reported that new records showed that the Department mislead the public about the release and that ICE's official statement—that the detainees were "low-risk offenders who do not have serious criminal records"—downplayed the risk to public safety.[310] USA Today reported that records obtained through a FOIA request show that among the detainees who were released included "one person in Texas charged with aggravated kidnapping and sexually assaulting a child, as well as others charged with armed assaults or assaulting police officers" while "another immigrant released from Miami had been charged with conspiracy to commit homicide."[311]

---

[304] GAO, "Secure Communities: Criminal Alien Removals Increased, But Technology Planning Improvements Needed," GAO-12-708, July 2012.
[305] DHS Office of Inspector General, ICE's Release of Immigration Detainees, August 2014, p. 38-39.
[306] Ibid.
[307] Ibid.
[308] Ibid.
[309] Ibid.
[310] Brad Heath, "U.S. misinformed Congress, public on immigrant release" USA Today, October 22, 2014.
[311] Ibid.

The decision by federal authorities to release illegal immigrants who had criminal records, including in some cases related to very violent charges, raises a question about the potential threat to public safety that results from the Department's lax approach to immigration enforcement. For example, the Center for Immigration Studies, a non-governmental organization that reports on immigration policy, published a review of enforcement statistics based on September 2014 data prepared by Immigration and Customs Enforcement. The Center for Immigration Studies reported: "The number of aliens who have received a final order of removal, but who are still in the United States, has risen to nearly 900,000. Nearly 167,000 of these are convicted criminals who were released by ICE and are currently at large."[312] Due to the potential threat to public safety, this should be a priority area of ongoing oversight by Congress and other watchdogs.

Evidence also suggests that ICE has struggled in executing its responsibilities under the Visa Security Program, which, according to the Inspector General, "is intended to prevent terrorists, criminals, and other ineligible applicants from receiving visas."[313] Under this program, DHS and ICE deploys personnel overseas to serve with U.S. officials from other agencies, including consular officers, to "provide expert advice," "review visa applications," and "conduct investigations with respect to consular matters under the jurisdiction of the Secretary of Homeland Security." [314] In 2014, the Inspector General identified a series of problems related to DHS's management of the Visa Security Program, including that participating officers did not have ready access to useful databases that are needed to vet applicants, that DHS and ICE does not effectively track hours and staff resources or data about investigation and screening outcomes to spot trends, and a lack of confidence in the program's performance measures. [315] These and other issues led the Inspector General to conclude that "ICE cannot ensure that the Visa Security Program is operating as intended." [316]

[312] Jessica M. Vaughn, "ICE Enforcement Collapses Further in 2014," Center for Immigration Studies, October 2014.
[313] DHS Office of Inspector General, "The DHS Visa Security Program," OIG-14-137, September 2014.
[314] Ibid.
[315] DHS Office of Inspector General, "The DHS Visa Security Program," OIG-14-137, September 2014.
[316] Ibid.

Homeland Security Investigations: ICE's Non-Immigration Enforcement Mission

ICE also has a broad mission that is not related to immigration enforcement.[317] As Kevin Abar, Assistant Special Agent in Charge of Homeland Security Investigations in New Mexico, explained to the Albuquerque Journal, "Too many people think we do immigration, and we don't really do any of that at all."[318]

Many of HSI's investigative missions, such as narcotics, weapons, financial, and cybercrime, overlap with the investigative jurisdiction of other federal law enforcement agencies with longer histories and more experience, such as the Federal Bureau of Investigations (FBI), the Bureau of Alcohol Tobacco, Firearms, and Explosives (ATF), the Drug Enforcement Agency (DEA), and the U.S. Secret Service. This raises important questions, including whether some of ICE's Homeland Security Investigation's responsibilities are duplicative, whether it is making a significant contribution to enforcing federal laws, or whether the responsibilities for enforcing these federal laws should be left to other agencies with primary jurisdiction and a longer history working in these areas.

ICE's investigative mission is largely a historical legacy of the merger of the U.S. Customs Service into DHS under the Homeland Security Act.[319] The U.S. Customs Service had a history that dates back to the nation's founding with responsibilities ranging from collecting import duties to prohibiting the import and commerce of illegal goods or items.[320] With DHS's creation, the majority of the U.S. Customs Service was transferred into Customs and Border Protection (CBP): however, Immigration and Customs Enforcement assumed the U.S. Customs Service's investigative arm.

In 2014, a review of HSI's investigative work raises many questions about whether their investigations are improving national security. For example, in October 2014, two HSI agents entered a women's lingerie store in Kansas City, Missouri. The agents purchased pairs of

---

[317] According to ICE Homeland Security Investigations: "HSI has broad legal authority to enforce a diverse array of federal statutes. It uses this authority to investigate all types of cross-border criminal activity, including: Financial crimes, money laundering and bulk cash smuggling; Commercial fraud and intellectual property theft; Cybercrimes ; Human rights violations; Human smuggling and trafficking; Immigration, document and benefit fraud; Narcotics and weapons smuggling/trafficking; Transnational gang activity; Export enforcement; and, International art and antiquity theft." For background on ICE and Homeland Security Investigations, see http://www.ice.gov/hsi, accessed December 28, 2014.

[318] Michael Coleman, "Mission Creep: Homeland Security a 'runaway train'", Albuquerque Journal, April 27, 2014.

[319] Overview, About ICE, Immigration and Customs Enforcement, at: http://www.ice.gov/about, December 31, 2014.

[320] About Homeland Security Investigations, Immigration and Customs Enforcement, at: http://www.ice.gov/hsi , December 31, 2014.

women's underwear that had a logo that was similar to that of the Kansas City Royals, which the store had recently produced to mark the team's success reaching the World Series. The store's co-owner told Committee minority staff: "We have a very strong hometown spirit here. We were really doing it because we were so excited about the team's success."[321] The agents then identified themselves to store owners by flashing their badges, and explaining that the merchandise infringed on Major League Baseball's copyright property.[322] The agents seized the store's remaining eighteen pairs of women's underwear.[323] The store's owner told Committee Staff that the agents accidentally left behind paperwork for a few moments before leaving the store, and returned moments later to collect it.[324] The store's owner noticed that the paperwork included an email communication from Major League Baseball about the merchandise, asking "Does this pass?"[325]

Enforcing intellectual property and copyright trademarks is one of Homeland Security Investigation's significant responsibilities and activities.[326] ICE reported opening nearly 4,000 cases related to Intellectual Property Rights enforcement in FY 2012 and FY 2013, leading to nearly 800 convictions.[327] Senator Coburn had asked ICE for statistics about the number of goods seized by ICE in the course of HSI investigations. While ICE "does not track counterfeit merchandise by type of merchandise seized," ICE provided joint statistics of annual intellectual property seizures by both CBP and ICE. In all, the two components made more than 28,000 seizures in FY2013.[328] Handbags and wallets accounted for 40 percent, the largest share, of ICE's commodity seizures, based on manufacturer's suggested retail price.[329] Altogether, ICE reports having a responsibility to enforce more than 80 laws related to intellectual property rights and trade fraud.[330] While many of these laws have a nexus to potential national security violations, and other crimes against U.S. citizens, Congress and the Department of Homeland Security should review these laws and ICE's allocation of investigative resources, particularly

[321] Committee minority staff phone call interview with a co-owner of Birdies of Kansas City, Missouri. October 24, 2014.
[322] Ibid.
[323] Ibid.
[324] Ibid.
[325] Ibid.
[326] Thomas S. Winkowski, Letter to Senator Tom Coburn and Enclosed White Paper, July 10, 2014.
[327] Ibid.
[328] Ibid.
[329] Ibid.
[330] Ibid.

given ICE's inability to effectively enforce the nation's immigration laws.

Potential National Security Vulnerabilities within DHS's Immigration Programs

While the primary missions of Immigration and Customs Enforcement and U.S. Citizenship and Immigration Services is to enforce immigration laws and administer the immigration system, both of these components have responsibilities for managing and overseeing unique immigration programs which are intended to draw specific populations of foreign immigrants or visitors into the United States. A review of the management of each of these programs raises troubling questions about DHS's management and whether these programs may be creating potential threats to national security.

The Student Exchange and Visitor Program (SEVP)

Immigration and Customs Enforcement is responsible for administering the Student Exchange and Visitor Program (SEVP), which is allowing 1.3 million students and visitors to stay in the United States in order to study or work.[331] SEVP is a post-9/11 security program instituted to register legitimate U.S. schools which can host foreign students and academics, and keep track of the foreign students and academics while they are in the United States. Schools apply to ICE to be permitted to host foreign students and must identify a designated school official (DSO) responsible for monitoring students on their campus, entering foreign students' information into an ICE database (SEVIS), and relaying information to DHS about the students' courses of study and attendance.[332] The SEVP program and SEVIS are operated based on fees, since schools must pay to be a part of the program and foreign students pay a fee for visa processing.[333]

One of the responsibilities that DHS and ICE must execute is monitoring the schools participating in the program.[334] In addition to the initial petition, schools enrolled in the SEVP must be recertified every two years by DHS. Unlike most other federal education programs,

[331] U.S. Immigration and Customs Enforcement, Student Exchange Visitor Program, "SEVIS by the Numbers: General Summary Quarterly Review, October 2014.
[332] "Student and Exchange Visitor Program, Immigration and Customs Enforcement Website, available at http://www.ice.gov/sevis/. Student and Exchange Visitor Program, Immigration and Customs Enforcement Website, available at http://www.ice.gov/sevis/, December 29, 2014.
[333] Ibid.
[334] Ibid.

schools do not need to be accredited or licensed to participate in the Student Exchange Visitor Program. Unaccredited or unlicensed schools may host students. ICE reports such schools undergo a special vetting process and are asked to provide additional information, such as letters from other institutions that such students and their credits are accepted at their institution. Flight schools must be FAA certified. According to the 2014 SEVP Quarterly Review, there are currently 8,988 schools enrolled in the SEVP program as of October 2014.[335]

Several oversight audits by the Government Accountability Office raised significant questions about ICE's management of the Student and Exchange Visitor Program, and whether it was vulnerable to fraud and abuse. In 2012, GAO reported that ICE "has not developed a process to identify and analyze program risks since assuming responsibility for [the program] in 2003" [336] and that ICE officials "have expressed concerns about fraud risks posed by schools that do not comply with [program] requirements."[337] A GAO audit identified examples of poor management of the program. Of particular concern was that 38 percent of the SEVP-certified flight schools eligible for the program did not have required FAA certifications.[338]

A follow-up audit by GAO in 2014 found that problems persisted with ICE's management of SEVP, specifically the "optional practical training" (OPT) component of the program which allows SEVP students to work in jobs related to their field of study.[339] GAO found that "ICE has not consistently collected the information and developed the monitoring mechanisms needed to help ensure foreign students comply with OPT requirements, thereby maintaining their legal status in the United States." [340] For example, GAO reviewed ICE's records on SEVP participants and found that the records of 38 percent (or 48,642 out of 126,796 visa holders) did not contain an employer's name. [341]

The problems identified by watchdog audits are substantiated by investigations and arrests that highlight the potential abuse and, in some cases, national security vulnerabilities

[335] U.S. Immigration and Customs Enforcement, Student Exchange Visitor Program, "SEVIS by the Numbers: General Summary Quarterly Review, October 2014.
[336] Government Accountability Office, Student and Exchange Visitor Program: DHS Needs to Assess Risks and Strengthen Oversight Functions, June 2012.
[337] Ibid.
[338] Ibid.
[339] Government Accountability Office, "Student and Exchange Visitor Program: DHS Needs to Assess Risk and Strengthen Oversight of Foreign Students with Employment Authorization," March 7, 2014.
[340] GAO, "Student and Exchange Visitor Program: DHS Needs to Assess Risk and Strengthen Oversight of Foreign Students with Employment Authorization," March 7, 2014.
[341] GAO, "Student and Exchange Visitor Program: DHS Needs to Assess Risk and Strengthen Oversight of Foreign Students with Employment Authorization," March 7, 2014.

associated with the SEVP. In March 2014, the founder of a California university, "Tri-Valley University," which was participating in SEVP, was convicted of 31 criminal counts, including "federal criminal counts, including wire fraud, visa fraud, and money laundering for her involvement in a large-scale visa fraud scheme."[342] In May 2014, the former head of a College Prep Academy in Georgia and a co-conspirator were sentenced for alien smuggling, according to the U.S. Attorney's Office of the Northern District of Georgia. Dong Seok Yi, the former head of the school, "conspired with Korean bar owners to enroll females into the school with the understanding that the females would not attend classes as required but would instead work in the bars, which are also known as room salons."[343]

Evidence also suggests that people plotting terrorist attacks have been in the United States using student visas. In October 2012, a student visa holder from Bangladesh was arrested for plotting to blow of the Federal Reserve Building in NYC.[344] That year, a Saudi man with a student visa was also arrested and convicted after "buying chemicals online and attempting to use a WMD" in Texas.[345] An ICE official told Committee staff that approximately 36 convicted terrorists came to the country using various forms of student visas.[346]

Given these risks and evidence showing ICE does not have strong oversight and accountability of this program, there is a risk that it could be exploited by foreign adversaries seeking entry into the United States to do harm, including terrorism, espionage, or engaging in other illegal activities, particularly given the imbalance between the program's scope and the resources that are dedicated to overseeing it. According to ICE officials, the agency has dedicated approximately 200 ICE agents assigned to overseeing the SEVP program,[347] which includes approximately 1.3 million visa holders and nearly 9,000 schools.[348] This means that, if responsibilities for overseeing the program are distributed evenly, each ICE agent must try to monitor approximately 6,500 students.

---

[342] ICE News Release, "President of Bay Area university convicted in student visa fraud scheme," March 24, 2014.
[343] ICE News Release, "Owner of Georgia English language school sentenced for immigration fraud." May 8, 2014.
[344] Josh Rogin, "State Department granted New York terror plotter a student visa," ForeignPolicy.com, October 18, 2012.
[345] Associated Press, "Saudi student found guilty in Texas terror plot," 2012.
[346] Minority committee staff interview with ICE HSI Special Agent Brian Smeltzer, Unit Chief, Counterterrorism and Criminal Exploitation Unit, July 1, 2014.
[347] Ibid
[348] Ibid.

EB-5 Visa Program

U.S. Citizenship and Immigration Services manages the Employment-Based Fifth Preference (EB-5) "Immigrant Investor" visa program. Congress created this program in the 1990s in order to encourage economic growth and investment in the United States.[349] One way that immigrant investors can earn a visa is by making a $500,000 or $1,000,000 investment into a USCIS-authorized "Regional Center," which pools immigrants' investments.[350] The Regional Centers are supposed to create at least 10 jobs per immigrant investor by making investments in new commercial enterprises that spur economic activity.[351]

USCIS is charged with the responsibility of overseeing this program—including approving each Regional Center's applications to become eligible to receive investments, vetting immigrant investors to ensure that they meet the program's eligibility requirements, and conducting background checks to ensure that they do not pose a risk to national security.

Growing the EB-5 program has been a priority for the Department of Homeland Security. Since 2009, participation in the EB-5 visa program has increased by nearly a factor of four—from 5,748 participants in 2008 to 22,444 EB-5 visa holders in 2014.[352] Meanwhile, the number of regional centers approved to participate has grown to at least 601.[353]

The White House has cited expanding the EB-5 program as a priority for encouraging economic growth. The President's Council on Jobs and Competitiveness issued an interim report recommending "five common-sense initiatives to boost jobs and competitiveness."[354] The Jobs Council stated "we need to fully subscribe and radically expand" the EB-5 program. The Jobs Council further declared, "If the EB-5 program reaches maximum capacity, it could result annually in the creation of approximately 4,000 new businesses[,] $2 billion to $4 billion of

[349] "EB-5 Immigrant Investor," U.S. Citizenship and Immigration Services, at: http://www.uscis.gov/working-united-states/permanent-workers/employment-based-immigration-fifth-preference-eb-5/eb-5-immigrant-investor, accessed December 31, 2014.
[350] Ibid.
[351] Ibid.
[352] United States Citizenship and Immigration Services, Number of I-526 Immigrant Petitions by Alien Entrepreneurs by Fiscal Year, Quarter, and Case Status 2008-2014, at: http://www.uscis.gov/sites/default/files/USCIS/Resources/Reports%20and%20Studies/Immigration%20Forms%20Data/Employmentbased/I526_performancedata_fy2014_qtr4.pdf, accessed December 10, 2014.
[353] U.S. Citizenship and Immigration Services, Immigrant Investor Regional Centers, http://www.uscis.gov/working-united-states/permanent-workers/employment-based-immigration-fifth-preference-eb-5/immigrant-investor-regional-centers.
[354] President's Council on Jobs and Competitiveness, "Taking Action, Building Confidence: Five Common-Sense Initiatives to Boost Jobs and Competiveness," Interim Report, The White House, October 2011.

foreign investment capital and create 40,000 jobs. But streamlining the application process and fully subscribing the program is just a start. Why have any cap on this kind of visa at all? Why not advertise it worldwide?"[355]

In 2013, Senator Chuck Grassley and Senator Coburn learned that the White House and National Security Staff (NSS) had apparently initiated an inter-agency review of the EB-5 program to examine potential vulnerabilities associated with the EB-5 program. The Senators obtained a draft document, which appeared to be written by or on behalf of the NSS, titled: "Forensic Assessment of Financial Flows Related to EB-5 Regional Centers."[356] The draft document stated that the "capital raising activities inherent in the regional center model raise concerns about investor fraud and other conduct that may violate U.S. securities laws" and "there is risk that EB-5 program participants may attempt to use the program as a tool or channel for money laundering, tax evasion, or other illicit financial conduct."[357] The NSS draft document reviewed cases of fraud and criminal activity in the program and wrote, "the case studies reveal that one of the primary vulnerabilities is that regional center developers may take immigrant investor money under false pretenses and fail to undertake or execute on the business plans presented to both the investors and USCIS. The consequences are also possible violations of federal immigration laws, securities laws, and criminal laws, in addition to possible state law violations."[358]

Besides the potential for fraud and financial-related crimes, the NSS draft document suggests that the White House's national security staff was also concerned about potential national security threats associated with the EB-5 program. The "Forensic Assessment" draft document included the following statement: "Vulnerabilities relating to possible infiltration by terrorist groups or foreign operatives are also before the NSS and being addressed separately by the interagency."[359] On October 18, 2013, Senator Tom Coburn sent a letter to National Security Advisor Ambassador Susan Rice that requested information about this draft document, the inter-agency review and its result. To date, she has not responded.

---

[355] Ibid, p.35.
[356] Forensic Assessment of Financial Flows Related to EB-5 Regional Center, Document Marked Deliberative and Pre-Decisional, National Security Staff.
[357] Ibid.
[358] Ibid.
[359] Ibid.

An additional review of the EB-5 program was prepared by U.S. Immigration and Customs Enforcement and Homeland Security Investigations at the request of the DHS Secretary.[360] The ICE-HSI review of the EB-5 program identified national security, criminal, and basic programmatic weaknesses in the EB-5 program, including the following vulnerabilities:

1. "Export of Sensitive Technology/Economic Espionage"
2. "Use by Foreign Government Agents/Espionage"
3. "Use by Terrorists"
4. "Investment Fraud by Regional Centers"
5. "Investment Fraud by Investors"
6. "Fraud Conspiracies by Investors and Regional Centers"
7. "Illicit Finance / Money Laundering" [361]

ICE's review of the EB-5 program, which was prepared at the request of the Secretary, concluded that the entire Regional Center model was too dangerous and should be scrapped: "Based on concerns outlined above, HSI made several suggestions for both legislative fixes and information collection fixes to close loopholes in the EB-5 program. The principal change proposed by HSI was that the Regional Center Model be allowed to sunset, as HSI maintains there are no safeguards that can be put in place that will ensure the integrity of the RC model."[362]

In December 2013, the Inspector General released a public report corroborating the weaknesses in USCIS's management of the EB-5 program that have been identified in the administration's internal reviews. [363] The Inspector General reported that: "USCIS is limited in its ability to prevent fraud or national security threats that could harm the U.S.; and it cannot demonstrate that the program is improving the U.S. economy and creating jobs for U.S. citizens as intended by Congress."[364]

Given the national security and criminal threats associated with the program, Senator

[360] Undated Memorandum, U.S. Customs and Immigration Enforcement on Implications of U.S. Immigration and Customs Case Against Procurement Agent. U.S. Immigration and Customs Enforcement, Homeland Security Investigations, "EB-5 Program Questions from DHS Secretary." Senator Grassley published a redacted copy of the document on his website, at: http://www.grassley.senate.gov/sites/default/files/issues/upload/EB-5-12-12-13-ICE-memo-security-vulnerabilities.pdf (Accessed: December 28, 2014).
[361] Ibid..
[362] Ibid.
[363] DHS Office of Inspector General, "United States Citizenship and Immigration Services' Employment-Based Fifth Preference (EB-5) Regional Center Program," OIG-14-19, December 2013.
[364] Ibid, p.1.

Coburn sought information from USCIS about how they were tracking the investments made through the EB-5 program to understand what economic impact it was having, specifically asking for information about regional centers' financials and investments. A DHS official told committee staff that DHS could not provide this information due to legal restrictions. However, even if it could, a DHS official explained that it would be impossible to do so: "while USCIS requires information about the job-creating company where the investment funds will ultimately be used to generate economic activity and create jobs, that information is not currently captured in any system of record," and, thus, "a thorough and complete list of investments would require the physical review of tens or hundreds of thousands of pages."[365] USCIS's use of a paper-based tracking system to oversee the EB-5 Regional Center program raises additional questions about the agency's ability to oversee the program.

Since USCIS was unable to provide information about the investments that were being made through the EB-5 program, Senator Coburn sent letters to the more than 430 regional centers that were listed on the USCIS website as approved to participate in the program as of March 10, 2014.[366] The information requested in these letters was intended to help inform Congress about the economic impact of the EB-5 regional center program, the roles and business activities of EB-5 regional centers, and the types of professionals providing services for EB-5 regional centers.

Approximately 53 percent (or 227 of 430) of the EB-5 regional centers did not provide any form of response. Roughly half of the 227 regional centers that did respond to the letter reported not receiving any EB-5 investments since their creation. Less than 60 Regional Centers disclosed either having received EB-5 investments or that they were awaiting USCIS approval of their B-5 investors' visa petitions. Of these, forty-three of the EB-5 regional centers that responded disclosed amounts of EB-5 investments received, which totaled an estimated $3.585 billion since the EB-5 program's creation in 1990. Twenty-one regional centers asserted

[365] Letter from DHS Office of Congressional Affairs to Senator Tom Coburn, August 23, 2013.
[366] Senator Coburn's office attempted to communicate with each of the Regional Centers in addition to sending letters. Senator Coburn's staff also attempted to phone call each of the Regional Centers that were listed on the USCIS website as approved for participating in the program. Some of the regional centers did not have websites, email addresses, or phone numbers available, so in a small minority of cases, staff was unable to communicate with an employee of the regional center to ensure that the letter was being sent to the appropriate address. The letters were sent to the e-mail and mailing addresses of EB-5 regional centers that were either confirmed over a telephone conversation, posted on the regional center's website, listed in the regional center's USCIS approval letter that is publicly posted, or obtained from corporate records searches.

that the information was confidential and proprietary. Ten regional centers provided responses that did not provide any of the information requested in Senator Coburn's letter.

Given the absence of compelling information or government oversight into how the EB-5 program is being used, it is unclear whether any economic benefit of the program justifies the criminal and national security risks associated with the program. Congress and DHS should eliminate or sunset the EB-5 visa program to mitigate these potential risks and to allow USCIS to refocus its efforts on administering the immigration system.

Conclusion

Evidence and the oversight work that has been done shows that DHS is not effectively administering and enforcing the nation's immigration laws. The Department has struggled to efficiently administer and vet immigration benefits requests. The Department has also failed to uphold the rule of law or enforce the nation's immigration's laws, increasing the probability of people seeking to enter the nation illegally, adding to the challenges of securing our borders. The Department also manages two immigration benefit programs which are vulnerable to fraud, abuse, and exploitation by potential national security threats.

As the lead agency with federal responsibilities for overseeing the nation's immigration systems, DHS must refocus and reprioritize its third mission. DHS must improve its administration of the immigration system and recommit to enforcing the rule of law to deter illegal immigration. This may be the area where DHS could make its most significant contribution to the nation's counterterrorism initiatives, including by vetting and tracking people who come to the United States to mitigate potential threats. The Department should reform, suspend, or end immigration benefit programs that are vulnerable to criminal and national security threats.

Mission 4—Safeguarding and Securing Cyberspace

Overview

In 2009, President Obama identified the basic challenge that the nation faces in cybersecurity. "It is the great irony of our Information Age—the very technologies that empower us to create and to build also empower those who would disrupt and destroy. And this paradox—seen and unseen—that we face every day," the President explained. "It is about the privacy and the economic security of American families," and also "a matter of public safety and national security."[367]

The cybersecurity threats facing our nation create a serious and persistent challenge, both to the private sector and the government. The American public is becoming accustomed to major data breaches or cyber attacks against commercial networks being reported in the national press. These incidents have become so commonplace that it has become almost cliché to repeat the frequent expression among cybersecurity experts that, "There are two kinds of organizations in the U.S.—those who know they've been hacked, and those who don't know they've been hacked."[368]

Less reported is the quiet but damaging nation-state sponsored or condoned economic or industrial espionage, including the theft of intellectual property or business information, through computer intrusions and data exfiltration that occurs on a daily basis. Former NSA Director General Keith Alexander called cyber espionage against the United States "the greatest transfer of wealth in history."[369] Estimates of the actual cost to the U.S. economy have ranged as high as hundreds of billions of dollars per year.[370]

The U.S. government also faces significant cybersecurity threats, including adversaries using weaknesses in our networks and information security systems to steal or disrupt sensitive

---

[367] The White House, "Remarks by the President on Securing Our Nation's Cyber Infrastructure," May 29, 2009.
[368] James Cook, "FBI Director: China Has Hacked Every Big US Company," Business Insider, October 6, 2014, at http://www.businessinsider.com/fbi-director-china-has-hacked-every-big-us-company-2014-10, accessed October 10, 2014.
[369] Josh Rogin, "NSA Chief: Cybercrime Constitutes the "Greatest Transfer of Wealth in History," FOREIGN POLICY (July 9, 2012), at http://thecable.foreignpolicy.com/posts/2012/07/09/nsa_chief_cybercrime_constitutes_the_greatest_transfer_of_wealth_in_history, accessed December 29, 2014.
[370] Office of the National Counterintelligence Executive, Foreign Spies Stealing U.S. Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage 2009-2011, p.4.

information, which can be used to weaken our government's defenses or to exploit citizens' personal information.

There is even a threat that adversaries could use cyber-attacks to disrupt or destroy information systems, including those that support the operations of critical infrastructure, to conduct real world damage, even potentially including loss of life. Former DHS Secretary Janet Napolitano publicly warned of the danger of a "cyber 9/11" attack and others have warned of "cyber Pearl Harbor".[371] These warnings may overstate the probability of such an attack. In 2014, DHS officials told Committee staff that it is "very difficult to kill people"[372] using cyber-attacks and that the greater concern of cyber-attacks on critical infrastructure is economic consequences. The potential for a cyber-attack that causes loss of human life remains a low-probability high-consequence event that must not be ignored.

The Department of Homeland Security has assumed significant responsibilities in the area of safeguarding and securing cyberspace. The Department defines this as its fourth priority mission: "DHS is responsible for protecting the federal executive branch civilian agencies and guiding the protection of the nation's critical infrastructure."[373] DHS currently operates extensive programs across several of its components and directorates focusing on cybersecurity, including programs within the National Protection and Programs Directorate ($696 million annually) and the U.S. Secret Service ($9.8 million annually), and ICE's Homeland Security Investigations component.[374] Overall, the Department spends nearly $706 million annually on cybersecurity-related federal programs.[375]

A review of DHS's cyber security programs raises questions about whether the Department is effectively fulfilling its cybersecurity mission, as well as whether its strategy for helping the nation safeguard and secure cyberspace is appropriate given the nature of the threats we face. First, the Department of Homeland Security has struggled to execute the responsibilities delegated to it by the Office of Management & Budget for improving the

[371] Reuters, "U.S. homeland chief: cyber 9/11 could happen "imminently"," January 24, 2013, at: http://www.reuters.com/article/2013/01/24/us-usa-cyber-threat-idUSBRE90N1A320130124.
[372] DHS officials briefing Committee Staff, April 17, 2014.
[373] "Department of Homeland Security Strategic Plan: Fiscal Years 2012-2016," Department of Homeland Security, February 2012.
[374] Memo from Congressional Research Service to HSGAC Minority Staff, "Historical Trends in FISMA Spending by Federal Agencies and Recent Cybersecurity Investments by the Department of Homeland Security, " November 13, 2014. Data on ICE-HSI expenditures related to cybersecurity was unavailable due to the structure of ICE-HSI and its funding.
[375] Id. As of FY2013, NPPD had 348 FTEs in these programs.

cybersecurity of federal civilian agencies. DHS has even struggled with its own information security practices and compliance with the Federal Information Security Management Act (FISMA), which is the federal statute that governs agencies' cyber security practices.[376] Second, it is unclear whether DHS's programs for assisting the private sector in preventing, mitigating, or recovering from cybersecurity incidents are providing significant value, and are worth taxpayers' investments in them.[377] Third, although DHS's law enforcement agencies involved in arresting cyber criminals are making a positive contribution, the Department's investment on law enforcement investigation of cybersecurity is likely a fraction of its spending on other cybersecurity programs. These findings raise a serious question of whether DHS's $700 million annual spending on cybersecurity programs could be put to better use to help the nation and private sector address the cybersecurity threats we face.

DHS Operational Responsibilities for Federal Civilian Cybersecurity

In 2010, the administration delegated operational responsibilities for overseeing federal civilian agencies' cybersecurity practices to DHS under FISMA, while maintaining OMB's overall management and budgetary authority. Four years after assuming this responsibility, and despite government-wide spending on cybersecurity exceeding $65 billion,[378] effective federal information security remains a significant challenge for an overwhelming majority of federal civilian agencies. GAO reported in September 2013 that the "inspectors general at 22 of 24 agencies cited information security as a major management challenge for the agency."[379] Protecting the federal government's information systems remains on GAO's high-risk list.[380]

Widespread weaknesses in the federal government's information security practices represent a significant vulnerability that could be exploited by adversaries, creating a potential threat to national security and American citizens. For example, in 2013, hackers gained access to U.S. Army Corps of Engineers network, and downloaded a non-public database of information

[376] Government Accountability Office, "Federal Information Security: Mixed Progress Implementing Program Components; Improved Metrics Needed to Measure Effectiveness," GAO-13-776. September 2013.
[377] DHS Office of Inspector General, "Implementation Status of the Enhanced Cybersecurity Services Program," OIG, 14-119, July 2014.
[378] Memo from Congressional Research Service to HSGAC Minority Staff, "FISMA Spending, Historical Trends," June 6, 2013.
[379] Government Accountability Office, "Protecting the Federal Government's Information Systems and Nation's Critical Infrastructures," GAO-13-283, February 14, 2013.
[380] Id.

about 85,000 dams, including sensitive security information and the potential fatalities that could be caused by a breach.[381] The Nuclear Regulatory Commission (NRC) stored sensitive cybersecurity details for nuclear plants on an unprotected shared drive, making them more vulnerable to theft.[382] In February 2013, hackers even breached the Federal Communications Commission's Emergency Broadcast System to broadcast warnings in Michigan, Montana, and North Dakota about a zombie attack.[383] Further, earlier this year, the Administration discovered that Chinese hackers had breached the U.S. Office of Personnel Management and one of its key security clearance investigation contractors.[384] The data targeted in both cases reportedly included information on federal employees with high-level security clearances. Then, in October, the White House revealed that hackers had breached its unclassified network, in an apparently state-sponsored attack.[385] It remains unclear what information the Russian hackers stole from the White House network.

The Department of Homeland Security is not solely or even chiefly responsible for poor cybersecurity across the federal government. The White House, including the Office of Management and Budget, and senior agency leaders ultimately must hold each agency and its personnel accountable for ensuring that federal networks and information systems are secure. However, evidence creates doubt that DHS's key programs for improving federal cybersecurity are yielding significant value.

National Cybersecurity Protection System (NCPS)

DHS's National Cybersecurity Protection System (NCPS) acts as an intrusion detection, analysis, information sharing, and intrusion prevention system for civilian federal networks; identifying suspicious traffic through analysis and comparison with signatures of known threats.[386] DHS achieves these four objectives in NCPS through three iterations of DHS's

[381] "The Federal Government's Track Record on Cybersecurity and Critical Infrastructure," A report prepared by the Minority Staff of the Homeland Security and Governmental Affairs Committee Sen. Tom Coburn, MD, Ranking Member February 4, 2014
[382] Ibid.
[383] Reuters, "Zombie Hack Blamed on Easy Passwords, February 14, 2013..
[384] Michael Schmidt, et al., "Chinese Hackers Pursue Key Data on U.S. Workers," New York Times, July 9, 2014; Ellen Nakashima, "DHS Contractor Suffers Major Computer Breach," Officials Say, Washington Post, August 6, 2014.
[385] Ellen Nakashima, "Hackers Breach Some White House Computers," Washington Post, Oct. 28, 2014.
[386] National Cybersecurity Protection System, Department of Homeland Security, at: http://www.dhs.gov/national-cybersecurity-protection-system-ncps, accessed December 31, 2014.

EINSTEIN software systems and threat analysis by cybersecurity experts at US-CERT. EINSTEIN 1 and 2 provide passive monitoring capabilities to detect suspicious traffic, and report it back to those analysts for review (and to develop new signatures).[387] EINSTEIN 3 Accelerated adds the ability to cut off intruders automatically when detected. However, none of the three versions of EINSTEIN has been deployed across all civilian federal networks.[388] The President requested more than $400 million to continue development of NCPS through Fiscal Year 2014.[389] In October 2014, OMB Director Shaun Donovan issued a memorandum for executive departments and agencies requiring them to enter into agreements with DHS to deploy Einstein.[390]

NCPS, however, also suffers from its share of problems. One of the key concerns about NCPS is that it relies heavily on signature-based detection—it operates by scanning traffic to and from federal networks for the fingerprints of known threats and vulnerabilities. Such systems can only protect against known threats, with the same fingerprints, and on traffic NCPS can see. So, for example, NCPS cannot protect against hackers that encrypt their traffic, because NCPS cannot decrypt that traffic to peer into it and look for bad actors and malware. Further NCPS cannot detect hackers if their software uses a vulnerability that has not been publicly revealed and DHS is not otherwise aware of—so called "zero days" (referring to the number of days a vulnerability has been publicly known)—or vulnerabilities that are too old to be included.[391] Finally, NCPS can only detect known fingerprints—malware that changes its signatures can be effectively impossible to detect by signature-based intrusion detection like NCPS.

For example, in March 2014, the Department's Inspector General found major flaws in how the Department of Homeland Security was managing NCPS, especially Einstein 3

[387] Hearing before the House of Representatives Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, on Examining The Cyber Threat To Critical Infrastructure And The American Economy, March 6, 2011.
[388] Id.
[389] President's Budget Request Fiscal Year 2014, Department of Homeland Security, National Protection & Programs Directorate, Network Security Deployment.
[390] Shaun Donovan, Memorandum for Heads of Executive Departments and Agencies, "Fiscal Year 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices," October 3, 2014.
[391] Like any computer software, intrusion detection systems including NCPS operate on servers with finite resources. Thus there is often an inherent conflict with intrusion detection systems between the desire to analyze and pass internet traffic on quickly (users do not want slow connections) and the desire to be as comprehensive as possible in looking for bad actors and malware (the more signatures that traffic has to be compared against, the slower the system works).

Accelerated, raising serious questions about the Department's ability to manage its existing responsibilities if codified, let alone new ones. Some of the problems the Inspector General identified in development of these systems included lack of performance measures and timelines, inadequate privacy protections, and minor vulnerabilities in Top Secret computer systems.[392]

The report concluded DHS's system of tracking contractors' performance in developing the NCPS lacked effective performance measures (clear milestones or deliverables) and timelines.[393] At the time of the report, DHS relied on a combination of vague "key performance parameters" that are difficult to quantify and an Integrated Master Schedule to monitor its progress.[394] Without these, the Inspector General said it would be "difficult for management to effectively monitor [EINSTEIN 3 Accelerated] implementation efforts. Further, there is little assurance that [DHS] would be able to deliver intrusion prevention capabilities to participating agencies on schedule."[395]

The Inspector General also found that DHS's operating procedures for handling individuals' personally identifiable information do not adequately protect that information. Specifically, the report concluded that DHS lacks specific instructions for how analysts should handle personally identifiable information, how they should minimize usage of it when it is unnecessary, and how to protect it on a day-to-day basis. Perhaps more troubling, DHS officials revealed to the Inspector General that the Privacy Impact Assessment DHS completed on the program overstates the training their analysts received in protecting individuals' privacy. The training itself is poorly documented. It is questionable from DHS's records whether it occurs at all and the Inspector General found that even if it did, those analysts might be unable to differentiate personally identifiable information from less- or non-sensitive data. Yet, they could be exposed to personal data on literally every American citizen as taxpayers submit their tax returns to the IRS, retirees receive their social security checks, and soldiers and veterans receive their salaries and retirement benefits.[396]

Finally, the Inspector General found "two minor vulnerabilities" in DHS's Top Secret systems that complement Einstein 3 Accelerated. According to the report, the vulnerabilities

[392] DHS Office of Inspector General, Implementation Status of EINSTEIN 3 Accelerated, OIG-14-52, March 2014.
[393] Id, p.7
[394] Id, p.8.
[395] Id, p.8.
[396] Id.

"are minimal and do not pose a significant threat to the safety and integrity of the system."[397] Nevertheless, these are the systems that DHS wants to run the federal government's firewall. If ever there was a system that should have perfect compliance, it would be this one.

Continuous Diagnostics & Mitigation (CDM)

Continuous Diagnostics & Mitigation (CDM) is DHS's approach to implement "continuous monitoring" of federal computer systems to enable real-time monitoring of cyber hygiene and FISMA compliance.[398] DHS hopes that CDM will provide a real-time picture of the vulnerabilities in a given agency's network—weak passwords, missing patches, antiquated operating systems like Windows XP, etc.—so that the agency can prioritize vulnerabilities for repair.

To implement the CDM program, DHS has partnered with the General Services Administration (GSA) to award a set of contracts intended for use across the federal government to implement the tools and services needed to achieve its vision. The contracts were awarded in August 2013 to seventeen different prime contractors with a potential combined ceiling value of roughly $100 billion over the five year period.[399] They allow federal agencies either to directly purchase, or use GSA to help purchase information technology products and services to, for example: discover unauthorized hardware or software on a network, assist with configuration management, manage network access, and monitor behavior on a network. CDM also allows agencies to track information resulting from the use of these monitoring tools on dashboards at the agency level, and at DHS.[400]

Implementing the collection of data and information through the dashboards at federal agencies is intended to provide DHS with a government-wide view of cyber threats and vulnerabilities as they evolve to improve situational awareness, a critical component of this

[397] Id., p.12.
[398] Continuous Diagnostics and Mitigation, Department of Homeland Security, at: http://www.dhs.gov/cdm, accessed December 31, 2014.
[399] Jason Miller, "DHS to standardize cyber protections through new contract," Federal News Radio, August 13, 2013.
[400] Continuous Diagnostics and Mitigation (CDM) Program Tools and Continuous Monitoring as a Service Blanket Purchase Agreement Ordering Guide 2014, available at http://www.gsa.gov/portal/mediaId/189495/fileName/CMaaS_Ordering_Guide_V40_Mar2014_v2.action, accessed December 31, 2014. .

program.[401] The contracts are structured such that the prices agencies pay for products and services underneath them include a built-in administrative fee of 2 percent that is intended to cover program administration costs at GSA.[402] At present, DHS is paying GSA for program administration of the contracts, but the idea is that over time, as more agencies use the contracts, the 2 percent fee included in the pricing will cover these costs.

In fiscal year 2014, DHS received $168 million to implement the CDM program, and requested an additional $142.6 million for fiscal year 2015.[403] The department's budget justification indicated that agencies were supposed to be purchasing and installing CDM capabilities during FY 2014. Despite the value DHS attributes to this program, as of early October, few agencies appear to have used these contracts to purchase goods or services. GSA has placed a small number of orders totaling roughly $59 million, most of which are in support of activities at DHS, rather than implementation at other agencies.[404] The International Trade Commission placed orders with SAIC under its CDM contract for software tools totaling $116,466 in July 2014.[405]

While patch management and cyber hygiene are clearly important, they are only basic security precautions, and are unlikely to stop a determined adversary, such as a nation state seeking to penetrate federal networks to steal sensitive information. There are also important questions about the implementation of CDM. The limited usage of these contracts to date calls into question whether and when DHS can successfully implement this component of its cybersecurity mission. It also means that DHS is paying program administration costs for contracts that, thus far, most of the rest of the federal government does not want to use.

[401] Department of Homeland Security National Protection & Programs Directorate Infrastructure Protection and Information Security Fiscal Year 2015 Congressional Justification at 44.
[402] Continuous Diagnostics and Mitigation (CDM) Program Tools and Continuous Monitoring as a Service Blanket Purchase Agreement Ordering Guide 2014, available at http://www.gsa.gov/portal/mediaId/189495/fileName/CMaaS_Ordering_Guide_V40_Mar2014_v2.action .
[403] Id at 46.
[404] Based on analysis of data from the Federal Procurement Data System-Next Generation as of October 2014.
[405] Id.

DHS's Struggles with its Own Information Security

Because it helps the Office of Management and Budget monitor cybersecurity and FISMA compliance for federal civilian agencies, one might expect DHS's own cybersecurity to be top notch, but a closer look shows that the Department suffers from many of the same shortcomings as other federal agencies.[406] OMB's devolution of operational authorities for federal civilian agencies' information security compliance to DHS puts the Department in the difficult position of trying to manage or direct its sister departments and agencies and hold them accountable for improving their cybersecurity practices. This despite that DHS is not setting a good example of effective cybersecurity, according to numerous audits by the DHS Inspector General and the Committee's oversight work.

For example, the Inspector General's recent audits of DHS's information security program identified widespread problems, including that patches were missing on several components' systems, including TSA's server containing biometric data on two million Americans.[407] In 2013, the Inspector General found that DHS was even failing to conduct basic security reviews to ensure that its classified systems were up-to-date and secure.[408] The Department doesn't effectively track security weaknesses it knows about, and doesn't fix them in time, sometimes taking years. DHS components are lousy at reporting security incidents when they happen. Many of the problems identified by the Inspector General have been cited in prior years' audits, and in some cases the IG's recommendations have been open for several years.[409] In December 2014, the Inspector General released its most recent audit of DHS's FISMA compliance. It reported that, once again, DHS "components are not consistently following DHS'[s] policies and procedures to update the system inventory and plan of action and milestones in the Department's enterprise management systems."[410] In one instance, the Inspector General reports that the Secret Service did not provide the Department's management with data required by OMB to evaluate the components' compliance; which represents a

[406] "The Federal Government's Track Record on Cybersecurity and Critical Infrastructure," A report prepared by the Minority Staff of the Homeland Security and Governmental Affairs Committee Sen. Tom Coburn, MD, Ranking Member February 4, 2014.
[407] Id.
[408] Office of Inspector General, "Evaluation of DHS' Information Security Program for Fiscal Year 2013," Department of Homeland Security, OIG-14-09, November 2013.
[409] Ibid
[410] Office of Inspector General, "Evaluation of DHS' Information Security Program for Fiscal Year 2014," Department of Homeland Security, OIG-15-16, December 12, 2014.

"significant deficiency" and hinders the Department's ability to monitor employees' compliance with information security rules.[411]

An alarming example of DHS's poor cybersecurity practices and failure to practice what the Department preaches came earlier this year during the countdown to Microsoft's April 2014 end-date for providing security patches and updates for its Windows XP software in April 2014, which had been originally announced in April 2012.[412] DHS's own US-CERT (which issues cybersecurity warnings to government and private sector partners) issued a warning in March alerting its subscribers of the danger of running Windows XP after April.[413] But as of November 2013, the Inspector General was warning that several of DHS's own components were still operating Windows XP. The Committee learned that the Department was continuing to run computers with the vulnerable software after Microsoft stopped providing updates, and after the Department's representatives had said it was no longer using the operating system.[414]

The Department has even struggled to effectively manage its responsibilities for ensuring that the best cybersecurity practices were used by the critical infrastructure entities that the Department itself manages. For example, in June 2014, GAO reported that DHS, through U.S. Coast Guard and FEMA, had not done enough to address potential cybersecurity weaknesses within our nation's ports, despite its recognition that ports are part of our nation's critical infrastructure.[415] GAO found that U.S. Coast Guard had "not conducted a risk assessment that fully addressed cybersecurity threats", and that FEMA was unable to ensure that cyber risks at U.S. ports were being effectively addressed.[416] In July 2014, a DHS Inspector General audit found that DHS's Domestic Nuclear Detection Office (DNDO) had not done enough to secure against potential cybersecurity vulnerabilities, including insider threats and the potential that

---

[411] Ibid.
[412] Stella Chernyak, Microsoft, Upgrade Today: Two-Year Countdown to End of Support for Windows XP and Office 2003, Windows Blog, http://blogs.windows.com/business/2012/04/09/upgrade-today-two-year-countdown-to-end-of-support-for-windows-xp-and-office-2003/, Apr. 9, 2012.
[413] Alert TA14-069A, Microsoft Ending Support for Windows XP and Office 2003, US-CERT (Mar. 10, 2014), available at https://www.us-cert.gov/ncas/alerts/TA14-069A-0, accessed December 29, 2014.
[414] E.g., Hearing before the Senate Committee on Homeland Security & Governmental Affairs on Strengthening Public-Private Partnerships to Reduce Cyber Risks to Our Nation's Critical Infrastructure. (Mar. 26, 2014) (Testimony of Phyllis Schneck and Post-Hearing Questions for the Record submitted to Phyllis Schneck)
[415] Government Accountability Office, "Maritime Critical Infrastructure Protection: DHS Needs to Better Address Port Cybersecurity," Government Accountability Office, June 2014.
[416] Government Accountability Office, "Maritime Critical Infrastructure Protection: DHS Needs to Better Address Port Cybersecurity," Government Accountability Office, June 2014.

insiders could steal sensitive data about nuclear systems through exfiltration.[417] The Inspector General also found that DNDO was not implementing "certain critical security patches"[418] or performing "wireless security scans of its facilities to identify non-DHS wireless access points operating within close proximity."[419]

Information Sharing and Critical Infrastructure Cybersecurity

DHS has also assumed responsibilities for leading federal and private sector cybersecurity information sharing and critical infrastructure protection. Both of these initiatives are led by the National Protection and Programs Directorate (NPPD) including its National Cybersecurity and Communications Integration Center (NCCIC). The Department has made progress in its efforts to share information with federal and private sector partners, and also to assist with the private sector. However, oversight of these programs has identified many areas where DHS continues to struggle to provide value with respect to these missions, and in some cases raises questions about the utility of several of DHS's cybersecurity programs.

National Cybersecurity & Communications Integration Center (NCCIC)

The National Cybersecurity and Communications Integration Center (NCCIC) is DHS's cybersecurity center.[420] It operates as a physical space and center to coordinate monitoring of cybersecurity and communications across civilian federal networks and critical infrastructure. It is home to many of DHS's cybersecurity programs, including the United States Computer Emergency Readiness Team and the National Cybersecurity Protection System.[421] The NCCIC floor has seats for representatives from numerous federal agencies including those in law enforcement and the intelligence community, as well as representatives from various companies operating critical infrastructure and their industry information sharing and analysis centers.

While this sort of central coordination is theoretically valuable, in practice it is not clear that DHS has achieved all that it can from this coordination, or an adequate level of

[417] DHS Office of Inspector General, "Domestic Nuclear Detection Office Has Taken Steps to Address Insider Threat, But Challenges Remain," July 2014, OIG-14-113.
[418] Ibid, page 12.
[419] Ibid, p.13.
[420] About the National Cybersecurity and Communications Integration Center, Department of Homeland Security, at: http://www.dhs.gov/about-national-cybersecurity-communications-integration-center, accessed December 31, 2014.
[421] Ibid.

participation. Audits of DHS's information sharing programs have identified key weaknesses that must be addressed for the Department to effectively fulfill its role coordinating federal cybersecurity information sharing. An October 2013 DHS Inspector General report determined that the NCCIC was struggling to serve as a hub of information for the other federal cybersecurity operations centers.[422] While the NCCIC had made some improvements, the IG found that DHS and the NCCIC struggled with "sharing cyber information among the Federal cyber operations centers."[423] The IG also reported that DHS's analysts at the NCCIC did not follow protocols during a recent cybersecurity incident simulation, including that "playbooks were underutilized," "which resulted in limited execution of appropriate operational actions."[424] The Inspector General also found that the National Protection and Programs Directorate had an outdated continuity of operations (COOP) plan, which may hinder its ability to "restore its mission-essential functions in the event of an emergency," when the NCCIC's information sharing services may be needed most.[425]

Technical Assistance

DHS's Computer Emergency Readiness Teams (CERT)—the United States Computer Emergency Readiness Team (US-CERT) and the Industrial Control Systems Computer Emergency Readiness Team (ICS-CERT) are DHS's response teams for investigating cybersecurity incidents, coordinating cyber information sharing, and providing cyber threat information to their customers.[426] They receive information from a variety of sources — from their on-site investigations, National Cybersecurity Protection System logs, submissions by the private sector, and classified intelligence reporting.

However, there are questions about the usefulness of DHS's effort to provide technical assistance and leadership for private sector critical infrastructure owners and operators to address potential cybersecurity threats. The Department has made progress developing

[422] DHS Office of the Inspector General, DHS' Efforts to Coordinate the Activities of Federal Cyber Operations Centers, October 25, 2013, OIG-14-02, available at http://www.oig.dhs.gov/assets/Mgmt/2014/OIG_14-02_Oct13.pdf, accessed December 29, 2014.
[423] Id, p.5.
[424] Id, p.13.
[425] Id, p.14.
[426] About the National Cybersecurity and Communications Integration Center, Department of Homeland Security, at: http://www.dhs.gov/about-national-cybersecurity-communications-integration-center, accessed December 31, 2014.

technical capabilities within its ICS-CERT office to analyze and assess potential vulnerabilities to computer-based process control systems that operate infrastructure systems.[427] However, there are open questions about how effectively DHS and NPPD are managing their efforts to partner with critical infrastructure sectors, as was discussed earlier in the report evaluating DHS's counterterrorism mission and information sharing with the private sector owners and operators of critical infrastructure.[428]

One concern about US-CERT's performance is that it does not always provide information nearly as quickly as alternative private sector threat analysis companies. For example, in March of this year, US-CERT issued an advisory that Google had released a critical update to its popular internet browser, Google Chrome.[429] But the advisory came days after Google announced it, and countless other private sector sources had already covered it—from popular news sites to small personal blogs.[430] The vulnerabilities fixed in the March 14 patch were critical security flaws publicly revealed in hacking competitions during the weekend between when Google issued the patch and US-CERT announced it.[431] Thus, those who relied on US-CERT to learn when to patch their browsers may have been exposed to hackers over the weekend.

Enhanced Cybersecurity Services (ECS)

Enhanced Cybersecurity Services (ECS) is DHS's cybersecurity information sharing service for the private sector, particularly critical infrastructure.[432] Through ECS, DHS shares many of the same threat indicators and signatures used in its National Cybersecurity Protection System with critical infrastructure owners and operators. The service, which is managed and offered as an add-on service by internet service providers, receives threat signatures that may not be publicly available from DHS and intelligence sources, in a similar manner to DHS's

[427] DHS Office of Inspector General, "DHS Can Make Improvements to Secure Industrial Control Systems," OIG-13-39, February 2013.
[428] Government Accountability Office, "Critical Infrastructure: Assessment of the Department of Homeland Security's Results of Its Critical Infrastructure Partnership Streamlining Efforts," GAO-14-100R, November 18, 2013.
[429] "Google Releases Security Updates for Chrome," US-CERT, March 18, 2014, available at https://www.us-cert.gov/ncas/current-activity/2014/03/18/Google-Releases-Security-Updates, accessed December 29, 2014.
[430] Google Chrome Releases Blog, Stable Channel Update, March 14, 2014, available at http://googlechromereleases.blogspot.com/2014/03/stable-channel-update_14.html, accessed December 29, 2014.
[431] Id.
[432] Enhanced Cybersecurity Services, Department of Homeland Security, at: http://www.dhs.gov/enhanced-cybersecurity-services, accessed December 31, 2014.

National Cybersecurity Protection System. Companies can then use those threat signatures to detect and block harmful network traffic.[433]

However, ECS also suffers from some of the same challenges as the National Cybersecurity Protection System, chiefly that it only protects against what we already know about. ECS does not protect us against the unknown threats, so-called "zero days" that a sophisticated adversary might use.[434] The Inspector General recently identified problems with DHS's management of ECS, including delaying the enrollment of critical infrastructure in the program, and providing less than useful threat signatures.[435] The Inspector General's report reveals that only three of the sixteen critical infrastructure sectors currently receive any ECS services, and that DHS has not enrolled any new participants in ECS since DHS took over the program from the Department of Defense in February 2013.[436] This is not due to lack of interest—some twenty-two prospective participants are waiting in the queue to join ECS—but because of an arduous eight-month eligibility and vetting process for prospective participants.[437] The report also revealed that ECS provides little added value in threat detection; providing the same threat indicators more than once, or threat indicators that are already available through unclassified sources like public reporting and commercial cybersecurity services..

ECS also presents a potential privacy concern. It includes a mechanism for private sector participants to send suspected threat data back to US-CERT on an automated basis, for analysis, if they choose. However, sending that data back to DHS presents privacy concerns if the data those participants send back includes individuals' personally identifiable information, such as data on the participating companies' employees or customers. For example, a local internet service provider or bank might "opt-in" to sending data back to DHS, without the consent of its customers whose personal data might be included in the package sent to DHS and its partner agencies.

[433] Ibid.
[434] The system relies on identifying and blocking known threat signatures.
[435] DHS Office of Inspector General, "Implementation Status of the Enhanced Cybersecurity Services Program," OIG, 14-119, July 2014.
[436] Ibid.
[437] Ibid.

Cybersecurity Crime and Enforcement

While the majority of DHS's cybersecurity funding and initiatives are housed with NPPD, and are focused on network security and defense, DHS also plays a role in federal law enforcement related to cybercrime. Specifically, the U.S. Secret Service has authority under federal law to investigate financial cybercrime, along with the Federal Bureau of Investigation. In April 2014 testimony before the Senate Homeland Security and Governmental Affairs Committee, a USSS official reported that, over the past four years, the Secret Service's cybercrime investigations "had resulted in over 4,900 arrests, associated with approximately $1.37 billion in fraud losses and the prevention of over $11.24 billion in potential fraud losses."[438] In July 2014, for example, the U.S. Secret Service arrested Russian-national Roman Valerevich Seleznev, who is considered to be "one of the world's most prolific traffickers of stolen financial information" and alleged to be involved in some of the most high-profile hacking incidents against American businesses in recent years.[439] In May 2013, the USSS closed an international payment processing systems that was alleged to have facilitated an estimated $6 billion in criminal money laundering. [440]

However, the USSS appears to be dedicating relatively few resources in the USSS's cybercrime enforcement investigations, with 260 "full time equivalents" and approximately $76 million devoted to cybercrime investigations in FY 2013.[441] The USSS reported to the Committee that "incrementally scaling the capacity of the Secret Service may provide proportional benefit in our efforts to investigate cyber criminals" and warned that the agency "continues to see growth in transnational cybercrime."[442]

ICE also devotes investigative resources to investigating cybercrime enforcement; Homeland Security Investigations reported making 2,492 cybercrime arrests in FY2014. [443] However, ICE explained to Committee staff that its cyber investigations largely focused on combatting "cyber-enabled" crime, which "refers to traditional transnational crimes, such as

[438] William Noonan, Testimony, Senate Homeland Security and Governmental Affairs Committee, April 2, 2014.
[439] "U.S. Secret Service Arrests One of the World's Most Prolific Traffickers of Stolen Financial Information," DHS, July 7, 2014.
[440] Responses of William Noonan, U.S. Secret Service, to Post-Hearing Questions for the Record from Senator Tom A. Coburn, April 2, 2014.
[441] Ibid.
[442] Ibid.
[443] DHS official email to Committee staff, November 12, 2014. ICE reported devoting 1,152,264 hours to cybercrime enforcement in FY2014.

smuggling and money laundering, which are substantially facilitated through the use of computers and computer networks."[444] This suggests that the amount of investigative resources that ICE devotes to investigating cyber espionage and crime is unlikely to significantly deter would be cyber criminals from attempting to attack and exploit networks.

Does DHS Have the Right Strategy to Safeguard and Secure Cyberspace?

One question that Congress and the Department must ask and consider is whether DHS is applying the right strategy for its initiatives to safeguard and secure cyberspace. Most of DHS's initiatives for cyber security are focused on mitigating vulnerabilities and improving cyber security defenses by trying to build stronger firewalls, and to encourage government and the private sector to adopt better cyber security practices to defend their networks. Yet, some computer security experts now question the usefulness of firewalling systems and other vulnerability mitigation tactics, since the most determined adversaries, including nation state actors, are likely to be able to defeat such defensive measures.

At a March 2014 committee hearing, Stephen Chabinsky, a cybersecurity expert and former senior FBI official, argued that the federal government should reorient its cyber security strategy from focusing on vulnerability mitigation to instead focus on deterrence.[445] Mr. Chabinsky explained that in the physical world, people wisely use vulnerability mitigations efforts (such as locking the doors and windows of our homes) to prevent criminal activity. But there is a limit to how much most people would invest in locks, hardened doors and windows, to prevent the most determined adversaries who might choose to seek entry into our homes. For example, reasonable people would not invest in all of the defensive measures that would be required to prevent a military force from breaking into their house. Instead, for physical security, Chabinsky explained, reasonable people adopt a strategy that largely relies on deterring the adversary, including by employing strategies like security systems and deploying law enforcement.[446] "When a monitoring company is alerted that a door was broken into at 3:00 in the morning, it calls the police to respond. It doesn't call the locksmith. And as a result, most

[444] Ibid.
[445] Testimony of Mr. Stephen Chabinsky, Senate Homeland Security and Governmental Affairs Committee, March 26, 2014.
[446] Ibid.

would be intruders are deterred from acting in the first place."[447] Mr. Chabinsky further warned that the public and private sector focus on vulnerability mitigation in cybersecurity may be a wasteful, and potentially could have the unintended consequence of making us even less secure by encouraging the development and proliferation of malware and other attack tools.[448]

Mr. Chabinsky is not alone in warning of the danger of a cybersecurity strategy that focuses too much on vulnerability mitigation. In 2010, Ms. Suzanne Spaulding, who would become the Under Secretary of the NPPD Directorate in 2013, eloquently warned about the dangers of vulnerability mitigation: "The promise of an impervious cybersecurity shield protecting vast amounts of information from a determined and sophisticated adversary is at best a distant dream, and at worst a dangerous myth."[449]

Another senior official at DHS has also suggested that increasing our focus on deterrence could yield security improvements by decreasing the incentives for adversaries to attack our networks. Mr. William Noonan, Deputy Special Agent in Charge with the U.S. Secret Service, told the Committee in his responses to questions for the record: "Current research on the cost of cybercrime indicates that preventing cybercrime through investigations, arrests, and deterrence is an effective means to reduce the aggregate economic cost of cybercrime."[450] Mr. Noonan further explained, "The risk of being caught certainly influences cyber criminals' decisions."[451]

Recognizing the limits of vulnerability mitigation—and that the idea of a cyber shield securing our networks is a dangerous illusion—and the understood benefit of deterring adversaries, Congress and the Department should fundamentally rethink DHS's strategy for safeguarding and securing cyberspace.

---

[447] Ibid.
[448] Ibid. Mr. Chabinsky went on to tell the Committee: "Making matters worse as industry and government agencies continue to spend greater resources on vulnerability mitigation, we find ourselves facing the problems of diminishing economic returns and perhaps even negative returns. With respect to diminishing returns, imagine trying to protect a building by spending millions of dollars on a 20-foot brick wall. Meanwhile, an adversary can go to a hardware store, and for less than $100, by a 30-foot ladder. That's happening every day in cyber, where defenses are expensive and malware is cheap. Far worse though is the concept of negative returns in which well-intentioned efforts actually make the problem worse. Consider our brick wall again. What if instead of buying a ladder, the adversary decides to use a life-threatening explosive to bring down the wall. This is not dissimilar from our current defensive cyber strategy which has had the unintended consequence of proliferating a greater quantity and quality of attack methods. Thereby, escalating the problem and placing more of our infrastructure at greater risk."
[449] Suzanne E. Spaulding, "No More Secrets: Then What?," Huffington Post, June 24, 2010.
[450] Responses of William Noonan, U.S. Secret Service, to Post-Hearing Questions for the Record from Senator Tom A. Coburn, April 2, 2014.
[451] Ibid.

Conclusion

Cyber attacks represent a serious and growing threat to the nation's security and prosperity. During recent years, the Department of Homeland Security has sought to emphasize the important roles that it has been assigned for safeguarding and securing cyberspace, both for the federal government and in concert with the private sector. However, a review of DHS's cybersecurity programs identifies serious challenges that the Department must overcome before it will succeed in executing its responsibilities or making a measurable difference in the security of the nation's information systems.

Mission 5—Strengthening National Preparedness and Resilience

Overview

DHS's fifth mission is to "strengthen national preparedness and resilience." To carry out this mission, DHS relies primarily on the Federal Emergency Management Agency (FEMA), which accounts for the largest share of DHS's annual budget. For fiscal year 2014, this amounts to $14 billion, or 23 percent out of a total departmental budget of $61 billion.[452]

Secretary Jeh Johnson discussed the resiliency mission repeatedly throughout the Fiscal Year 2015 budget hearings, stating that "DHS also must be vigilant in preparing for and responding to disasters, including floods, wildfires, tornadoes, hurricanes, and most recently, chemical leaks like the 2014 spill into the Elk River in West Virginia that threatened the water supply of hundreds of thousands of people."[453] The Assistant Secretary for Infrastructure Protection recently said the Department has "moved not only from a security focus to a resiliency focus," in commenting on DHS's role in protecting infrastructure from the effects of climate change.[454]

This expansion of FEMA's mission, combined with inherent structural flaws in the programs FEMA uses to prepare for and respond to natural disasters and other threats, has led to increasing expenditures with little evidence to show that the nation is better off. In fact, a review of FEMA's programs and their effectiveness raises serious questions about the extent to which they are making our nation better prepared for, or more resilient to, disasters. Since 2002, DHS has spent $170 billion on FEMA and its programs, of which $37.6 billion was related to Hurricane Katrina.[455] Much of this spending is focused on subsidizing state, local, and private sector spending on emergency management and public safety, including through homeland security grants, after-the-fact disaster relief assistance for events that occurred weeks, months,

[452] Department of Homeland Security, Congressional Budget Justification FY 2015, Volume I, FY2014 Enacted Column, pg. 10 and 13, includes funding for the Disaster Relief Fund and the National Flood Insurance Program, available at http://www.dhs.gov/sites/default/files/publications/DHS-Congressional-Budget-Justification-FY2015.pdf .
[453] Written testimony of DHS Secretary Jeh Johnson for the House Committee on Appropriations, Subcommittee on Homeland Security hearing on DHS' FY2015 Budget Request, March 11, 2014.
[454] Lisa Anderson, "US Homeland Security moves to tackle climate change risks," Reuters, September 25, 2014.
[455] Analysis of appropriations, obligations, and net outlays for the Federal Emergency Management Agency from 2002 to 2013 performed by the Congressional Research Service.

years, or in some cases even decades ago, and subsidized property insurance for those who live in flood zones.

On the preparedness side, the agency now administers a suite of grant programs that effectively function as federal block grants to subsidize parochial state and local priorities.[456] Special interests that benefit from these dedicated streams of federal funding have and will likely continue to fight efforts to reform and streamline these grants to help refocus them around true counterterrorism priorities.

On the recovery side, federal resources should be dedicated to helping rebuild and recover from our most severe disasters, not small disasters that qualify for federal funding because of a flawed quirk in our policies.[457] After the immediate response and recovery activities following a disaster are over, FEMA's dedicated employees effectively become insurance adjustors, engaging in administrative back and forth with state and local entities to rebuild public infrastructure, tying both sides up in needless red tape at the expense of taxpayers who foot the bill.

In similar fashion, Congress has once again turned its back on fiscal discipline and sound actuarial policy by rolling back reforms to the National Flood Insurance Program.[458] One of the most basic ways to improve resilience is to discourage people from living in our most flood-prone areas through insurance rates that reflect true risk. Yet, this year, Congress rolled back planned rate increases to the program, further jeopardizing the program's fiscal condition, while increasing the future payments taxpayers will bear to rebuild homes and infrastructure in places where they should not be.

Few Americans would disagree that there is a role for the federal government to step in and provide aid to state and local communities after a natural disaster or terrorist attack to help save lives and repair our communities. Most Americans can remember an event that wrought destruction upon fellow citizens. From Hurricane Katrina and Super-storm Sandy to the tornados that devastated Joplin, Missouri and Moore, Oklahoma, the American public knows

---

[456] See earlier discussion about homeland security grants in the section of this report evaluating DHS's counterterrorism mission.

[457] "An Imperfect Storm: How Outdated Federal Rules Distort the Disaster Declaration Process and Fleece Taxpayers," Senator Tom Coburn, U.S. Senate Homeland Security and Governmental Affairs Committee, December 31, 2014.

[458] Congressional Research Service, Bill Summary of H.R. 3370, available at https://www.congress.gov/bill/113th-congress/house-bill/3370 .

too well the kind of destruction and tragedy that natural disasters can leave in their wake. Therefore, the nation is thankful that an organization like FEMA is on call to provide help when serious disasters strike. FEMA has improved its ability to quickly mobilize and provide assistance in response to disasters since Hurricane Katrina.[459] It is precisely because of the critical role that FEMA plays in our darkest hours that Congress must look to its current challenges in order to identify, and enact, meaningful reforms.

FEMA: Preparing Our Nation

Since 2002, FEMA has awarded $38.2 billion under grant programs that provide money to state and local governments, port and transit agencies, nonprofits, and other groups to improve preparedness.[460] FEMA defines preparedness through the National Preparedness Goal, released in 2011, as: "A secure and resilient nation with the capabilities required across the whole community to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk."[461] FEMA defines these risks within DHS' "all hazards" framework as natural disasters, disease pandemics, chemical spills and other manmade hazards, terrorist attacks and cyber-attacks.[462]

The agency provides state and local governments with grant funding to enhance their capacity to prepare, prevent, and respond to these different threats. The largest of these is the Homeland Security Grant Program, which includes three components: the State Homeland Security Grant Program (SHSGP), with $9.8 billion in awards, the Urban Areas Security Initiative (UASI) with $7.9 billion in awards, and Operation Stonegarden, with $376.4 million in awards since 2002.[463] SHSGP provides funding to states to implement and develop capabilities identified in their homeland security strategies, while UASI provides funding to high-density,

[459] For example, during Hurricane Sandy, FEMA pre-positioned commodities and assets, activated response centers, and deployed over 900 personnel ahead of Sandy's landfall. The total personnel surged to nearly 7,500 people two weeks later. The number of personnel deployed during Sandy exceeded the total deployed for Hurricanes Isaac and Irene combined. Federal Emergency Management Agency, Hurricane Sandy After-Action Report, July 1, 2013, pg.4,5 available at http://www.fema.gov/media-library-data/20130726-1923-25045-7442/sandy_fema_aar.pdf

[460] Federal Emergency Management Agency, National Award Summary Report Data as of May 15, 2014.

[461] Federal Emergency Management Agency, National preparedness Goal, available at http://www.fema.gov/national-preparedness-goal

[462] Ibid

[463] Federal Emergency Management Agency, National Award Summary Report Data as of May 15, 2014.

high-threat urban areas throughout the country to prevent and respond to terrorist threats.[464] Operation Stonegarden provides funds to facilitate border security activities.[465]

While these programs are well-intentioned, the simple fact is that there is little concrete evidence proving that the billions of dollars poured into them have made us safer. To the contrary, evidence shows that, more than 13 years after the 9/11 attacks, these programs are marked by three basic flaws: the programs are not truly risk-based, as was recommended by the 9/11 Commission; FEMA does not provide effective oversight of how grant funds are used; and FEMA and DHS continue to lack a concrete ability to effectively measure performance of grants. Combined, these flaws mean that rather than having a narrow, focused program that funds the highest priority projects needed to prevent terrorism, we are continuing to sponsor, year after year, programs that have effectively become nothing more than an expensive subsidy to state and local law enforcement, public safety, and emergency management.

Failure to Implement a True Risk-Based Approach to Preparedness Grants

As is often the case, DHS and FEMA's inability to fully implement a risk-based approach to administering the Homeland Security Grant Program starts with Congress. When the Homeland Security Act of 2002 established the Department, it included provisions that moved the Office of Domestic Preparedness into DHS from the Department of Justice, and brought along with it legacy programs intended to address state and local preparedness.[466] The 9/11 Commission detailed one of the major flaws with the grant programs, as they existed at that time, which was the fact that "a major portion of the billions of dollars appropriated for state and local assistance is allocated so that each state gets a certain amount, or an allocation based on its population…"[467] The Commission recommended that:

> Homeland security assistance should be based strictly on an assessment of risks and vulnerabilities…We understand the contention that every state and city needs to have some minimum infrastructure for emergency response. But federal homeland security

[464] U.S. Department of Homeland Security, Funding Opportunity Announcement (FOA), FY2014 Homeland Security Grant Program, pg.4, available at http://www.fema.gov/media-library-data/1395161200285-5b07ed0456056217175fbdee28d2b06e/FY_2014_HSGP_FOA_Final.pdf

[465] Ibid

[466] Public Law 107-296, Title IV, Subtitle C, §430 and Congressional Research Service, "Department of Homeland Security Assistance to States and Localities: A Summary and Issues for the 111th Congress," R 40246, April 30, 2010, pg. 2.

[467] "The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States," July 22, 2004, pg. 395-396, available at http://govinfo.library.unt.edu/911/report/index.htm .

> assistance should not remain a program for general revenue sharing. It should supplement state and local resources based on the risks and vulnerabilities that merit additional support. **Congress should not use this money as a pork barrel**.[468] [emphasis added].

Despite this recommendation, Congress enshrined the statutory allocation of a minimum level of grant funding under the SHSGP to all 50 states, as well as American Samoa, the Commonwealth of the Northern Mariana Islands, Guam, and the Virgin Islands with passage of the Implementing Recommendations of the 9/11 Commission Act of 2007.[469] For FY 2014, this means that, at a minimum, 17.8 percent of the total program funding has to be allocated before risk, or any other factor, including ability to effectively manage grant funding, is taken into account.[470]

In 2013, the DHS Office of Inspector General issued a series of reports evaluating the ability of the island territories to manage grants awarded under the HSGP. The reports demonstrate the problems inherent in requiring a statutory minimum allocation of grant funding.[471] For example, the OIG found that American Samoa did not assess its risks and vulnerabilities, did not measure progress in achieving needed capabilities, and did not comply with federal training and exercise requirements, property management, or accounting for personnel time charges.[472] In 2011, the territory indicated in its application to FEMA, called an investment justification, which is supposed to detail the specific projects on which grant funds will be used, that it planned to fund a project called "Multi Discipline Border Control" for

---

[468] Ibid, p. 396.
[469] Public Law 110-53, Title I, § 2004(e).
[470] Based on the statutory requirement to allocate at least 0.35% of total funding to each of the 50 states and 0.08% to each of the four Pacific island territories as outlined in Public Law 110-53, Title I, § 2004(e).
[471] In addition to the example discussed above, the OIG has also Identified problems with grant management in the Commonwealth of the Northern Mariana Islands, Guam, and the Virgin Islands. The findings in these reports ranged from a failure to report data to FEMA on grant expenditures, to, in the case of the Virgin Islands, the award of a sole source contract for planning activities worth $472,167 for which the agency could produce no supporting documents to show that it received deliverables. See U.S. Department of Homeland Security Office of Inspector General, "The Commonwealth of the Northern Mariana Islands' Management of Homeland Security Grant Program Awards for Fiscal Year 2009 Through 2011," OIG-14-05, November 2013, http://www.oig.dhs.gov/assets/Mgmt/2014/OIG_14-05_Nov13.pdf ; U.S. Department of Homeland Security Office of Inspector General, "Guam's Management of Homeland Security Grant Program Awards for Fiscal Year 2009 to 2011," OIG-14-06, November 2013, http://www.oig.dhs.gov/assets/Mgmt/2014/OIG_14-06_Nov13.pdf; U.S. Department of Homeland Security Office of Inspector General, "The U.S. Virgin Islands' Management of State Homeland Security Program Grants Awarded During Fiscal Years 2007 through 2009," OIG-12-29, January 2012, http://www.oig.dhs.gov/assets/Mgmt/OIG_12-29_Jan12.pdf .
[472] U.S. Department of Homeland Security Office of Inspector General, "American Samoa's Management of Homeland Security Grant Program Awards for Fiscal Year 2009-2011," OIG-14-16, December 2013, pg. 1, available at http://www.oig.dhs.gov/assets/Mgmt/2014/OIG_14-16_Dec13.pdf

$609,576.[473] Its application provided no clear indication of what was actually needed or what specific capabilities would be acquired, but indicated that the Territory would spend $20,000 on planning, $20,000 on organization, and $569,576 for "unspecified equipment."[474] Despite these weaknesses, the Territory has received a total of $18.9 million in funds under the SHSGP since 2002, an effect of the presence of statutory minimums required by law.[475]

The Implementing Recommendations of the 9/11 Commission Act of 2007 also required the Administrator of FEMA to identify high-risk urban areas that will be eligible for funding under the UASI program based on an assessment of the threat of, vulnerability to and consequences of a terrorist act.[476] As discussed in an earlier section of this report, Senator Coburn issued a report on homeland security grants in December of 2002, which detailed examples of how UASI grant funds were spent in 15 different cities.[477] The report catalogued the growth of the number of urban areas receiving funding through the program over time. In the pre-9/11 version of the grant program, 7 urban areas received funding. [478] In 2010, the program had grown to provide funding to 64 different urban areas, coinciding with its highest funding level after 9/11.[479] As funding declined in subsequent years, so did the number of urban areas included in the program, coming back down to a total of 39 jurisdictions for FY 2014.[480] Changes in funding levels and changes in the results of FEMA's analysis of threats, vulnerabilities, and consequences produce winners and losers in who receives grant funding, and this fact has led to significant lobbying efforts on the part of those in Congress to ensure that their jurisdictions stay in the black, regardless of the extent to which a true terrorist threat exists.[481]

---

[473] Ibid at pg. 11.
[474] Ibid at pg. 11.
[475] Federal Emergency Management Agency, National Award Summary Report Data as of May 15, 2014.
[476] Public Law 110-53, Title I, § 2003(b).
[477] Senator Tom Coburn, "Safety at Any Price: Assessing the Impact of Homeland Security Spending in U.S. Cities," December 2012, available at http://www.coburn.senate.gov/public/index.cfm?a=Files.Serve&File_Ibid=b86fdaeb-86ff-4d19-a112-415ec85aa9b6
[478] Ibid at p. 14.
[479] Ibid at pg. 15 and see Federal Emergency Management Agency, National Award Summary Report Data as of May 15, 2014.
[480] Federal Emergency Management Agency, Fiscal Year 2014 UASI/SHSP Allocations.
[481] Senator Tom Coburn, Safety at Any Price: Assessing the Impact of Homeland Security Spending in U.S. Cities, December 2012, available at http://www.coburn.senate.gov/public/index.cfm?a=Files.Serve&File_Ibid=b86fdaeb-86ff-4d19-a112-415ec85aa9b6

Failure to Provide Effective Oversight of Grant Spending

While FEMA's allocation mechanism provides some measure of taking risk into account in determining which urban areas will receive funding, it does not mean that grant funding actually goes towards projects that reduce those risks and make us safer. This is because the states and urban areas that receive program funds exercise significant discretion in deciding what to purchase with their grant funds, as long as they meet FEMA's broad requirements on what is allowable under the program. As discussed earlier in this report, Senator Coburn's 2012 report, "Safety at Any Price: Assessing the Impact of Homeland Security Spending in U.S. Cities", identified many questionable grant expenditures under the UASI program.[482]

In December 2012, the U.S. Senate Permanent Subcommittee on Investigations (PSI) released a report evaluating federal support for fusion centers, which are locally-run, multi-agency organizations to facilitate the sharing of information and intelligence to prevent terrorist attacks and crime in the United States.[483] DHS uses the Homeland Security Grant Program as the primary funding mechanism to provide funding to fusion centers. The PSI report further detailed problems with the grants, including the use of funding for activities that had little to do with counterterrorism activities. Examples included the purchase of Chevy Tahoes for a local Fire Department official, equipment for a surveillance monitoring room used in criminal investigations, laptops for the county medical examiner, shirt-button cameras, and cell-phone tracking devices, and a new records management system for a city police department.[484]

In the last example, city officials ultimately used the grant funds to purchase items that were very different from those identified in their original application to FEMA.[485] When asked about it, a senior FEMA official confirmed at the time that, as long as the expenditures were ultimately allowable, states could purchase something different from what was indicated in their applications.[486] A more recent GAO report identified $60 million in funding that states

[482] Ibid.
[483] United State Senate Permanent Subcommittee on Investigations, Committee on Homeland Security and Governmental Affairs, "Federal Support for and Involvement In State and Local Fusion Centers," Majority and minority Staff Report, October 3, 2012, http://www.hsgac.senate.gov/download/report_federal-support-for-and-involvement-in-state-and-local-fusions-centers .
[484] Ibid at pgs. 71-81.
[485] Ibid at pgs. 80-82.
[486] Ibid at pg. 82.

identified in their grant applications as being incorrectly related to fusion centers when it was not, confirming that this problem still exists.[487]

FEMA and DHS's fiscal stewardship of the grant programs has also been problematic. On February 13, 2012, then-DHS Secretary Napolitano provided guidance through FEMA to its state partners identifying strategies FEMA was to use to expedite the spending of $8.3 billion in unspent grant funding available from prior years.[488] These strategies were based around allowing grantees to apply funds to "more urgent priorities;" expanding allowable costs under some programs; and waiving program requirements in some cases. The guidance noted that the effort to move money quicker was in response to the "need for fiscal stimulus," a tacit acknowledgement that the grant programs are as much about pumping money into states as they are about bolstering counterterrorism efforts. The grant guidance did not acknowledge that even some portion of this $8.3 billion in unspent taxpayer dollars may not have been needed at the time if states couldn't find a way to spend it, and could have potentially be recovered. At the same time that billions of dollars in funding were unspent, FEMA was requesting an additional $1.5 billion in new funding for the preparedness grant program in fiscal year 2013.[489]

Although FEMA has since shortened the period of performance on its preparedness grants from three years to two years in an effort to ensure that funds are spent more quickly, the problem of unspent grant funding remains. As of May 2014, a total of $4.8 billion in funding across all of FEMA's preparedness grants remained unspent.[490]

Failure to Develop and Implement Objective Performance Metrics

Beyond an inability to ensure that grant funding is allocated towards our highest-priority and highest-risk needs, the GAO and the DHS OIG have repeatedly noted that FEMA lacks concrete performance measures for its preparedness grants. In June 2012, the OIG issued a report which found that:

---

[487] Government Accountability Office, "Information Sharing: DHS is Assessing Fusion Center Capabilities and Results, but Needs to More Accurately Account for Federal Funding Provided to Fusion Centers," GAO-15-155, November 2014, at Highlights, available at http://www.gao.gov/assets/670/666760.pdf .

[488] Department of Homeland Security, "Guidance to State Administrative Agencies to Expedite the Expenditure of Certain DHS/FEMA Grant Funding," February 13, 2012.

[489] Department of Homeland Security, Federal Emergency Management Agency, State and Local Programs Fiscal Year 2013 Congressional Justification at pg. SLP-3, available at https://www.fema.gov/pdf/about/budget/11b_fema_state_local_programs_dhs_fy13_cj.pdf .

[490] Federal Emergency Management Agency, National Funding Fact Sheet Summary Data as of May 15, 2014.

> FEMA did not have a system in place to determine the extent that Homeland Security Grant Program funds enhanced the states' capabilities to prevent, deter, respond to, and recover from terrorist attacks, major disasters, and other emergencies before awarding more funds to the states. FEMA did not require states to report progress in achieving milestones as part of the annual application process for Homeland Security Grant Program fund[s]. As a result, when annual grant application investment justifications for individual continuing projects were being reviewed, FEMA did not know if prior year milestones for the projects had been completed. FEMA also did not know the amount of funding required to achieve needed preparedness and response capabilities.[491]

Later that year, and again in December 2013, the OIG noted that the states also had weaknesses in having measurable performance goals to guide their grant awards.[492]

In March 2011, GAO reported that FEMA's efforts to develop and implement a comprehensive, measurable, national preparedness assessment of capability and gaps were not yet complete and suggested that Congress consider limiting preparedness grant funding until FEMA completes a national preparedness assessment of capability gaps based on tiered, capability-specific, performance objectives to enable prioritization of grant funding.[493] In March 2013, GAO testified that FEMA still had not yet established clear, objective, and quantifiable capability requirements and performance measures that are needed to identify gaps.[494] GAO went on to note that FEMA's attempts to measure performance of its grants through production of a National Preparedness Report, as well as production of state-level preparedness reports, has not been sufficient because these efforts have primarily relied on self-reported, unverified data.[495]

FEMA points to states' more recent implementation and usage of Threat and Hazard Identification and Risk Assessments (THIRA) as a key part of its process to better measure

---

[491] DHS Office of Inspector General, "The Federal Emergency Management Agency's Requirements for Reporting Homeland Security Grant Program Achievements," OIG-12-92, June 2012, at pg. 1, available at http://www.oig.dhs.gov/assets/Mgmt/2012/OIG_12-92_Jun12.pdf .

[492] DHS Office of Inspector General, "Annual Report to Congress on States' and Urban Areas Management of Homeland Security Grant Programs Fiscal Year 2012," OIG-13-18, December 2012, at pg. 4-5, available at http://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-18_Dec12.pdf and DHS Office of Inspector General, "Annual Report to Congress on States and Urban Areas' Management of Homeland Security Grant Programs Fiscal Year 2013," OIG-14-22, December 2013, at pg. 3, available at http://www.oig.dhs.gov/assets/Mgmt/2014/OIG_14-22_Dec13.pdf .

[493] Government Accountability Office, "Managing Preparedness Grants and Assessing National Capabilities: Continuing Challenges Impede FEMA's Progress," GAO-12-526-T, March 20, 2012.

[494] Government Accountability Office, "National Preparedness: FEMA Has Made Progress in Improving Grant Management and Assessing Capabilities, but Challenges Remain," GAO-13-456T, March 19, 2013, p.11.

[495] Ibid at pg. 11-12.

performance.[496] The THIRA is a document completed by the states that identifies the risks the state faces, and then maps those risks to one of 31 "core capabilities" developed by FEMA that are "the distinct critical elements needed to achieve the [National Preparedness] Goal." [497] States are then supposed to target the use of grant funding to projects that improve the capabilities needed to address the identified threats and risks.[498]

Like the previous state-level preparedness reports, however, the THIRAs rely on self-reported data and information from the states. In addition, the "core capabilities" states are supposed to achieve are in many cases, extremely broad, and ill-suited for objective measurement. For example, one of the capabilities is "economic recovery," defined as the ability to "return economic and business activities to a healthy state and develop new business and employment opportunities that result in a sustainable and economically viable community."[499] Another involves the protection of natural resources.[500] Another involves strengthening the resilience and security of the supply chain.[501] Perhaps the broadest measure of them all involves developing the capability to engage in planning, defined as the ability to "conduct a systematic process engaging the whole community in the development of executable strategic, operational, and/or community-based approaches to meet defined objectives."[502]

It would be impossible to ever objectively determine how good a state is at planning, how well it can strengthen the supply chain (what is being supplied is not detailed in the measure), or whether it has gained the full capability for economic recovery. There is no feasible way for FEMA to tell a state that it has developed "enough" of such broad capabilities, meaning that states will be able to effectively justify the expenditure of grant funds in perpetuity, based on self-reported needs, and self-reported progress. Finally, the inclusion of such broad capabilities also serves to highlight how far a grant program that was originally intended to be focused on counterterrorism has strayed.

---

[496] Ibid. at pg. 12.
[497] Federal Emergency Management Agency, "Threat and Hazard Identification and Risk Assessment," available at https://www.fema.gov/threat-and-hazard-Ibidentification-and-risk-assessment and "Core Capabilities" available at http://www.fema.gov/core-capabilities .
[498] U.S. Department of Homeland Security, Funding Opportunity Announcement (FOA), FY2014 Homeland Security Grant Program, at pg. 4, available at http://www.fema.gov/media-library-data/1395161200285-5b07ed0456056217175fbdee28d2b06e/FY_2014_HSGP_FOA_Final.pdf .
[499] Federal Emergency Management Agency, "Core Capabilities" available at http://www.fema.gov/core-capabilities
[500] Ibid.
[501] Ibid.
[502] Ibid.

Disaster Resilience

The Robert T. Stafford Emergency Relief and Disaster Assistance Act lays out the authorities granted to the President to declare major disasters and trigger FEMA's implementation of a number of different programs intended to help individuals recover and to rebuild damaged publicly-owned infrastructure.[503] These programs are paid for out of the Disaster Relief Fund (DRF), an account FEMA oversees and for which annual funding is determined by FEMA's estimates of spending plans for all past disasters, as well as the 10-year rolling average cost of past disasters.[504] Following major disasters like Hurricanes Katrina and Sandy, Congress has also passed supplemental appropriation bills to provide additional funding.[505] From 1989 to 2014, Congress has appropriated a total of $169.2 billion to the DRF to pay for the costs of recovery.[506]

The federal government's failed response to Hurricane Katrina marked a watershed low point, particularly for DHS and FEMA. A report issued by the Senate Homeland Security and Governmental Affairs Committee in 2006 stated unequivocally that, "FEMA was unprepared for a catastrophic event the scale of Katrina," and "DHS failed to effectively lead the federal response to Katrina."[507] Since that low point, FEMA has made improvements in a number of areas, most notably in its ability to provide more effective immediate response following a disaster, and in its ability to speed payments to individuals affected by a disaster, while decreasing instances of improper payments.

These improvements, however, are dwarfed by continued significant structural challenges to the way FEMA manages its disaster programs. The first is that the flawed mechanism FEMA and the President rely on to declare federal disasters results in the declaration of too many disasters, triggering the use of federal recovery programs in instances where states and local government should recover on their own. The second is that FEMA's Public Assistance program—which pays to rebuild facilities owned by state and local government entities and by certain nonprofits—represents the largest share of disaster recovery

[503] Public Law 93-288; and see Congressional Research Service, "FEMA's Disaster Relief Fund: Overview and Selected Issues," R43537, May 7, 2014 at Summary.
[504] Ibid at pg. 6-7.
[505] Ibid at pg. 4-5.
[506] Ibid at pg. 9.
[507] "Hurricane Katrina: A Nation Still Unprepared," Special Report of the Committee on Homeland Security and Governmental Affairs, United States Senate, at pg. 6, available at http://www.gpo.gov/fdsys/pkg/CRPT-109srpt322/pdf/CRPT-109srpt322.pdf

funding. The program ties FEMA, its funding recipients, and the DHS Inspector General up in disputes about what to pay for and what not to pay for that can drag on for years.

Excessive Declaration of Federal Disasters

In 1988, Congress made clear federal aid should be provided only when "the disaster is of such severity and magnitude that effective response is beyond the capabilities of the state and the affected local governments and that federal assistance was needed to save lives and property."[508] Despite this, FEMA's methodology for declaring disasters leads taxpayers to foot the bill to rebuild communities in many instances that most people would not consider to be severe disasters where state and local capabilities have been overwhelmed. The main indicator FEMA uses has not been consistently updated over time, is biased towards declaring disasters in small population states, and allows states to game the system when they over-estimate the amount of damage in the immediate aftermath of a storm.

Though regulations outline six factors for FEMA to consider when recommending a declaration, GAO found FEMA primarily relies on one—the statewide per capita damage indicator.[509] In 1986, prior to the passage of the Stafford Act, FEMA proposed the idea of using a statewide per capita damage indicator as a means of gauging the fiscal capacity of a jurisdiction affected by a disaster.

In simple language, FEMA takes the total estimated dollar amount of damage that occurs after a storm or disaster, divides it by the population[510] of the state where the disaster occurred, and then determines whether this per-capita amount is above a certain threshold (the per capita indicator). FEMA's 1986 proposal utilized $1 based on the 1983 national per capita income of $11,667.[511] In fiscal year 2013, the per capita indicator was $1.37 – meaning, a state with 10 million people would have to incur more than $13.7 million in estimated eligible damage for FEMA to recommend Public Assistance funding.[512] However, FEMA did not adjust the indicator for

[508] 42 U.S. Code § 5170 - Procedure for declaration
[509] U.S. Government Accountability Office "Improved Criteria Needed to Assess Jurisdictions Capability to Respond and Recover on Its Own,", GAO-12-838, September, 2012, pg. 24; http://www.gao.gov/assets/650/648162.pdf .
[510] Population data is based on the latest Census, which at present was conducted in 2010.
[511] 51 Fed. Reg. 13,332 (Apr. 18, 1986)
[512] Federal Emergency Management Agency, see http://fema.ideascale.com/a/ideas/recent/campaign-filter/byids/campaigns/59618 .

inflation for the years between 1986 and 1999.[513] As a result, the indicator has only risen 37 percent, from $1.00 to $1.37, since 1986. Meanwhile, inflation over that period would have increased the indicator from $1 of damage to $2.15 in 2014.[514]

GAO analyzed actual and projected obligations for 508 disaster declarations which received Public Assistance grants during fiscal years 2004-2011.[515] It found that fewer disasters would have been declared had FEMA updated the indicator to consider increases in personal income or price inflation for all of the years since 1986. Specifically, GAO found that nearly half—a full 44 percent—of those disasters would not have met the threshold indicator if the indicator had been adjusted for changes in income, and that 25 percent would have failed to qualify had the per capita damage indicator been adjusted for inflation.[516]

The use of the per capita damage indicator also creates a bias in favor of declaring disaster in small-population states. Because the indicator is determined by dividing the dollar amount of damage by the state's population, a state with a low population can meet FEMA's threshold of $1.37 with a lower amount of damage than a state with a larger population. For example, in 2013, a major winter storm hit a broad part of the northern Texas and southern Oklahoma. Both states applied for disaster relief. The estimated amount of damage in Oklahoma was $6.4 million, which amounted to a statewide damage indicator of $1.70, which met FEMA's per capita damage threshold, and led to a declaration covering a number of counties that border Texas.[517] The preliminary damage assessment for the same winter storm in Texas was $30 million,[518] which fell $5 million short of the number needed to get Texas above the per capita damage indicator. As a result, FEMA denied Texas's request for a major disaster declaration in

[513] U.S. Government Accountability Office, "Improved Criteria Needed to Assess Jurisdictions Capability to Respond and Recover on Its Own," GAO-12-838, September, 2012, pg. 24, http://www.gao.gov/assets/650/648162.pdf

[514] "CPI Inflation Calculator," http://data.bls.gov/cgi-bin/cpicalc.pl, accessed May 23, 2014.

[515] U.S. Government Accountability Office, "Improved Criteria Needed to Assess Jurisdictions Capability to Respond and Recover on Its Own," GAO-12-838, September, 2012, , pg. 24; http://www.gao.gov/assets/650/648162.pdf,.

[516] U.S. Government Accountability Office "Improved Criteria Needed to Assess Jurisdictions Capability to Respond and Recover on Its Own,", GAO-12-838, September, 2012, , p. 24; http://www.gao.gov/assets/650/648162.pdf,.

[517] "Oklahoma – Sever Winter Storm," FEMA.gov, January 30, 2014; pg. 2, http://www.fema.gov/media-library-data/1393619267269-e777eab6d237c9da9fce6405e2c9107a/PDA+Report+FEMA-4164-DR-OK.pdf, .

[518] "Texas Severe Winter Storm – Denial of Appeal," FEMA, April 15, 2014; http://www.fema.gov/media-library/assets/documents/95015,.

counties near the Oklahoma-Texas border affected by the storm, stating "the impact from the event was not of the severity and magnitude that warrants a major disaster declaration."[519]

Finally, states often over-estimate damage, which increases the number of inaccurate "disaster" declarations. Even under FEMA's current outdated model, 43 percent of all 2011 and 2012 disasters would not have been declared had a more accurate estimate been provided in the preliminary damage assessment reports. For example, in June 2012, Oklahoma received a disaster declaration for tornadoes, straight line winds and floods.[520] The preliminary damage estimate was $5.9 million, exceeding the state's damage threshold by about $840,000.[521] However, two years later, FEMA has only obligated $2.7 million in disaster-related projects, or $3.2 million under the original estimate.[522] If a more accurate estimate of damage was considered, FEMA would not have recommended a disaster declaration. States in similar situations have no incentive under the current rules to provide an accurate assessment, but rather to push estimates as high as possible to trigger disaster declarations to receive federal funding.

Improvements to Emergency Response, With Continued Problems

Particularly when compared to the response following Hurricane Katrina, FEMA demonstrated significant improvements in its response to Hurricane Sandy in October 2012. For example, during the response, FEMA employed WebEOC, an online crisis management system to coordinate and support response operations.[523] This system was used by FEMA and its federal partners for activities ranging from resource requests from the field to tracking assistance delivered to survivors. According to FEMA's After Action Report, the use of a single online platform for information sharing contributed to a more unified federal response. Despite

[519] "FEMA Denies 15 North Texas Counties Disaster Assistance for the Second Time," KXII, April 24, 2014; http://www.kxii.com/news/headlines/FEMA-denies-15-North-Texas-counties-disaster-assistance-for-the-second-time-256098441.html,.
[520] "Oklahoma – Severe Storms, Tornadoes, Straight Line Winds, and Flooding," FEMA, June 14, 2012; http://www.fema.gov/media-library-data/20130726-1846-25045-1600/dhs_ocfo_pda_report_fema_4064_dr_ok.pdf, accessed June 3, 2014.
[521] "Oklahoma – Severe Storms, Tornadoes, Straight Line Winds, and Flooding," FEMA, June 14, 2012; http://www.fema.gov/media-library-data/20130726-1846-25045-1600/dhs_ocfo_pda_report_fema_4064_dr_ok.pdf, accessed June 3, 2014, p. 2. Note: Threshold is 2010 statewide population of 3,751,351multiplied by $1.35
[522] "Open FEMA Dataset: Public Assistance Funded Projects," FEMA, April 3, 2014; https://www.fema.gov/data-feeds/openfema-dataset-public-assistance-funded-projects-details-v1; accessed May 24, 2014.
[523]Federal Emergency Management Agency, Hurricane Sandy After-Action Report, July 1, 2013, at pg. 9, available at http://www.fema.gov/media-library-data/20130726-1923-25045-7442/sandy_fema_aar.pdf, .

being the first deployment of the WebEOC system, sixty percent of the National Recovery Coordination Center personnel rated the system as being "effective" or "very effective" during Hurricane Sandy.[524]

FEMA also noted that Hurricane Sandy was one of the largest and most diverse personnel deployments in FEMA history.[525] Over 900 FEMA staff pre-deployed before Hurricane Sandy made landfall, and about a month after the storm, FEMA deployed 9,971 people. [526] In early 2013, staff from the Committee on Homeland Security and Governmental Affairs visited New York and New Jersey, and FEMA's pre-deployment of personnel prior to the storm, and ability to surge and increase the number of people deployed afterwards was a strength frequently cited by state and local community officials.[527] FEMA's ability to more quickly deploy staff was the result of changes made in 2011 to its program for training and deploying its "reservist" staff, which calls upon trained individuals to support recovery operations, and is distinct from FEMA's full-time employed staff.[528]

Following Hurricane Sandy, FEMA was able to direct disaster assistance payments to those affected by the storm more quickly when compared with the rate at which other federal agencies disbursed funding through other recovery programs. In January of 2013, Congress approved $50 billion in supplemental disaster funding for 19 different federal agencies.[529] In July of 2013, roughly nine months after the storm, FEMA had fully disbursed about $4 billion dollars, compared with less than half a billion spent by all other agencies tasked with recovery.[530] At the same time, FEMA made progress in reducing the rate of improper payments, i.e. those that are made to individuals or organizations who are not eligible to receive them, particularly when compared to Hurricane Katrina. After Hurricane Katrina, GAO identified $1 billion in potentially improper payments, a rate of 16 percent of the total payments made to individuals.[531] Following Hurricane Sandy, GAO found that the potential rate of improper payments dropped

[524] Ibid at pg. 9; The National Recovery Coordination Center is FEMA's hub for co-locating personnel from different federal agencies involved in the response.
[525] Ibid at pg. 30.
[526] Ibid. at 30.
[527] Staff interviews with state and local officials in New York and New Jersey.
[528] Ibid at 30.
[529] Congressional Research Service, Summary Report: Congressional Action on the FY2013 Disaster Supplemental, R42892, February 20, 2013.
[530] Hurricane Sandy Rebuilding Task Force, Monthly Public Financial Update, August 19, 2013, pg. 5.
[531] GAO, Hurricanes Katrina and Rita Disaster Relief: Improper and Potentially Fraudulent Individual Assistance Payments Estimated to be Between $600 Million and $1 Billion, GAO-06-844T, June 14, 2006, Highlights page, http://www.gao.gov/new.items/d06844t.pdf .

drastically, and identified an estimated $39 million in potentially improper payments, or about 2.6 percent of the total amount of individual assistance.[532] GAO still identified additional steps FEMA should take to continue to improve and reduce the improper payments rate further. Yet, FEMA's recent track record demonstrates significant improvements in this area.

Despite these strengths and progress, work still remains for FEMA to successfully accomplish the goal of effective emergency response. For example, the largest deployment in FEMA's history came at a price. The deployment nearly exhausted the number of available personnel. By November 12, FEMA had deployed 44 percent of its permanent employees.[533] First-time deployed staff reported confusion with the deployment process and confusion providing services.[534] State and local officials in New York and New Jersey consistently said that, while FEMA had a significant presence, its staff and reservists were often unable to answer questions related to FEMA's recovery programs. Further, FEMA encountered many challenges with such a large deployed workforce, including having no facility to stage personnel as they began deploying to the field, lack of information technology for personnel, as well as challenges providing lodging for its staff.[535]

Additionally, FEMA experienced the challenge of integrating federal senior leader coordination and communications into response and recovery during the Hurricane Sandy response. According to FEMA, they along with their Federal partners "experienced challenges with accurately, clearly, and quickly communicating senior leaders' decisions to those responsible for implementing them and to those affected by them."[536] The Hurricane Sandy After-Action Report gave the example of a temporary 100-percent federal cost share for some services in order to expedite disaster recovery. However, there was a challenge getting the specifics to staff responding to the storm.[537] Similar issues surrounding lack of communication and confusion has been noted by the DHS-OIG in the past. For example, during an oversight deployment to the Oklahoma City Joint Field Office, the DHS-OIG observed instances where

[532] U.S. Government Accountability Office, "Hurricane Sandy: FEMA Has Improved Disaster Aid Verification but Could Act to Further Limit Improper Assistance," GAO-15-15, December 2014, Highlights page.
[533] Ibid at p. 33.
[534] Federal Emergency Management Agency, "Hurricane Sandy FEMA After-Action Report," July 1, 2013, http://www.fema.gov/media-library-data/20130726-1923-25045-7442/sandy_fema_aar.pdf, pg. 33 http://www.fema.gov/media-library-data/20130726-1923-25045-7442/sandy_fema_aar.pdf,
[535] Ibid at p. 34.
[536] Ibid at pg. 10.
[537] Ibid at pg. 10

FEMA personnel provided incomplete and, at times, inaccurate information to Public Assistance applicants regarding Federal procurement standards.[538] The audit further noted that this was not a surprise because previous audit reports and personal observations have shown similar instances have been occurring for several years.[539] Strengthening FEMA's workforce should remain an ongoing area for focus and oversight.[540]

Inefficiency in Long Term Recovery Programs

FEMA's public assistance program, which is used to rebuild state and local and nonprofit facilities as well as other projects, accounts for the lion's share of FEMA's disaster funding. Since 1998, FEMA has obligated more than $58 billion on public assistance projects.[541] FEMA implements this program through grants made to the states, which then award sub-grants to other state or local entities, as well as certain types of nonprofits, to reimburse them for the cost of repairing disaster-damaged facilities.[542] To be eligible for repayment, the damage has to have been the direct result of the disaster.[543] FEMA will repay 75 percent of the total cost to repair a damaged building that meets the eligibility guidelines, or, if the cost to repair the building is more than 50 percent of the total cost to replace it, FEMA will repay 75 percent of the total replacement cost.[544] There are three significant problems that have contributed to

---

[538] U.S. Department of Homeland Security, Office of the Inspector General, FEMA's Progress in Clarifying its "50 percent rule" for the Public Assistance Grant Program," OIG-14-123D, Washington D.C. August 2014. http://www.oig.dhs.gov/assets/Mgmt/2014/OIG_14-123-D_Jul14.pdf

[539] Ibid. In 2014, GAO has also reported on opportunities to strengthen and increase the effectiveness of FEMA's workforce management. Specifically, GAO reviewed FEMA human capital management efforts in 2012 and 2013 and has made a number of related recommendations, many of which FEMA has implemented, and some of which are still underway. U.S. Government Accountability Office, "Federal Emergency Management Agency: Opportunities to Achieve Efficiencies and Strengthen Operations," GAO-14-687T, July 24, 2014, Highlights.

[540] In 2014, GAO has also reported on opportunities to strengthen and increase the effectiveness of FEMA's workforce management. Specifically, GAO reviewed FEMA human capital management efforts in 2012 and 2013 and has made a number of related recommendations, many of which FEMA has implemented, and some of which are still underway. U.S. Government Accountability Office, "Federal Emergency Management Agency: Opportunities to Achieve Efficiencies and Strengthen Operations," GAO-14-687T, July 24, 2014, Highlights.

[541] Federal Emergency Management Agency, Open FEMA Dataset: Public Assistance Funded Project Details – V1, https://www.fema.gov/data-feeds/openfema-dataset-public-assistance-funded-projects-details-v1, accessed December 30, 2014.

[542] FEMA, "Public Assistance: Local, State, Tribal and Non-profit: available at https://www.fema.gov/public-assistance-local-state-tribal-and-non-profit, accessed November 26, 2014.

[543] FEMA, "Public Assistance: Eligibility," available at https://www.fema.gov/public-assistance-eligibility, accessed November 26, 2014.

[544] U.S. Department of Homeland Security, Office of the Inspector General, FEMA's Progress in Clarifying its "50 percent rule" for the Public Assistance Grant Program," OIG-14-123D, Washington D.C. August 2014. http://www.oig.dhs.gov/assets/Mgmt/2014/OIG_14-123-D_Jul14.pdf , accessed December 31, 2014.

increased costs and inefficiency in FEMA's management of this program over time: poor application of the 50 percent rule, decisions to pay for ineligible costs, and its failure to close out disasters in a timely manner.

In August of 2014, the DHS-OIG issued a report highlighting the continued need for FEMA to fix its approach to applying the 50 percent rule.[545] This decision is critical, because when FEMA decides to pay for the cost to replace a building instead of just repairing it, it leads to a potentially significant increase in the cost to the taxpayer. Although the problems with applying this rule have been documented over a long period of time, the DHS-OIG highlighted the significance in light of Hurricane Sandy. According to the report, FEMA made 15 repair or replace decisions in New York and New Jersey totaling just under $6 million based on a 50 percent policy that FEMA admitted was "in need of significant review and revision."[546] In a number of different reports, the OIG found that FEMA often failed to document their decisions, used "conceptual" instead of actual cost estimates to determine how much repair or replacement would cost, and failed to determine whether the costs the agency would pay for were reasonable, which is a requirement under the program.[547]

In 2012, the DHS Inspector General found that FEMA, through faulty application of this rule, decided to pay to replace facilities at the University of Iowa damaged in floods in 2008 instead of just to repair them, resulting in excess costs of $83.7 million that the agency refused to get back, despite a recommendation from the OIG to do so.[548] Notably, at the time FEMA made its decision, using faulty information, it estimated that the cost to replace one of the facilities in question was only $50 million, yet years later, the cost ballooned to $300 million.[549] Because the program works on a cost reimbursement basis, with the federal government paying for at least 75 percent of a project's total costs, the state and local organizations have little incentive to control costs once FEMA makes this initial, often erroneous, determination, leading taxpayers to foot the bill for costs that should not be covered at all.

---

[545] Ibid.
[546] Ibid, p..4.
[547] Ibid.
[548] U.S. Department of Homeland Security, Office of the Inspector General, FEMA's Decisions to Replace Rather than Repair Buildings at the University of Iowa, DD-12-17, June 2012, pg. 18, available at http://www.oig.dhs.gov/assets/GrantReports/OIG_DD-12-17_Jun12.pdf, accessed December 31, 2014.
[549] Ibid at p. 21.

Beyond this, FEMA's administration of public assistance rebuilding grants is problematic in other ways. In December 2008, the GAO reviewed the use of public assistance grants to fund rebuilding projects after Hurricane Katrina and Rita, which at the time was estimated at nearly $11 billion.[550] GAO identified problems in determining what damage to facilities was actually caused by the disaster and in estimating costs; problems with effectively sharing information between federal, state, and local officials; problems with FEMA reversing its own decisions after applicants had already begun work on approved projects; and problems with having enough experienced and knowledgeable staff to effectively administer the program.[551]

Following Hurricane Sandy, Senator Coburn's staff met personally with state and local officials in New York and New Jersey in early 2013 that were in the process of implementing public assistance-funded projects with FEMA.[552] Across the board, those individuals noted the same significant problems that echoed the GAO's findings, albeit 5 years later, in getting accurate and straight answers from FEMA's staff on specific program questions. A number of the applicants hired contractors to help them navigate the complexities of the program because they could not do it on their own. That is as much an indication as any that this program is in need of reform.

Finally, the time it takes to close out a disaster is not only a financial strain on taxpayers, but is an indicator of how rapidly an area has fully recovered from a disaster. The requirements to "close out" a disaster are established in 44 C.F.R. 13.50. However, FEMA considers a disaster and/or emergency closed when all of the applicant's projects are completed and the applicant's expenses have been reconciled.[553] According to FEMA, over 800 disasters are currently open with ongoing recovery and mitigation projects.[554] Moreover, there are currently 40 open

[550] GAO, Disaster Recovery: FEMA's Public Assistance Grant Program Experienced Challenges with Gulf Coast Rebuilding, GAO-09-129, Washington DC, December 2008, Highlights page, http://www.gao.gov/assets/290/284493.pdf, accessed December 31, 2014.
[551] Ibid at Highlights.
[552] Committee staff visit to New York, March 11-March 13, 2013; Committee staff visit to New Jersey, February 6-7, 2013.
[553] Congressional Research Service, Federal Emergency Management: A Brief Introduction, R42845 Washington, D.C.; November 30, 2012.
[554] U.S. Department of Homeland Security, Office of the Inspector General, Annual Performance Plan for Fiscal year 2014. Washington, D.C., pg. 22 http://www.oig.dhs.gov/assets/PDFs/OIG_APP_FY14.pdf

disasters that are over 10 years old.[555] One of the oldest open disasters is the Northridge Earthquake, the 6.7 magnitude that rocked the San Fernando Valley region of Los Angeles, California over twenty years ago in 1994.[556] By not closing out disasters, federal dollars are tied up in old disasters when those funds could be put to better use and fund current or future disasters and ensure timely response during an emergency.

There is also little compliance with existing laws that limit the time on recovery spending, according to the OIG.[557] The Inspector General has consistently noted issues with FEMA internal controls relating to disaster recovery, including the lack of internal controls for timely disaster close out, resulting in disasters remaining open for a long time..[558] The Congressional Research Service has also reviewed the disaster closeout process and noted that Stafford Act recovery is not subject to strict deadlines.[559] By not enforcing the deadline regulations, FEMA is incentivizing federal disaster assistance recipients to drag out recovery. FEMA's policies are actually inhibiting DHS's fifth mission of ensuring rapid recovery from a catastrophic event.

Flood Insurance

Floods are among the most destructive hazards facing the nation. The federal government, in partnership with private insurers and servicing contractors, is the primary provider of flood insurance in the United States. Currently, the National Flood Insurance Program (NFIP) covers more than 5 million households and businesses across the country with nearly $1.3 trillion in risk exposure, according to FEMA as of October 2014.[560]

The significant risk related to floods makes insuring against floods costly. After a string of natural disasters, Congress established the NFIP through passage of the National Flood

[555] Senate Homeland Security and Governmental Affairs analysis of FEMA Disaster Declarations Summary - Open Government Dataset: http://www.fema.gov/media-library/assets/documents/28318?Ibid=6292; FEMA data Un-Liquidated Obligations- Financial Information Tool, as of September 23, 2014.
[556] http://www.theatlantic.com/infocus/2014/01/the-northrIbidge-earthquake-20-years-ago-today/100664/
[557] U.S. Department of Homeland Security, Office of the Inspector General, Opportunities to Improve FEMA's Disaster Closeout Process OIG-10-49, Washington, D.C.; Jan. 2010 http://www.oig.dhs.gov/assets/Mgmt/OIG_10-49_Feb10.pdf
[558] Ibid at pg.6.
[559] Congressional Research Service, Federal Emergency Management: A Brief Introduction, R42845 Washington, D.C.; November 30, 2012.
[560] Federal Emergency Management Agency, "Flood Insurance Statistics for the Current Month," available at https://www.fema.gov/flood-insurance-statistics-current-month

Insurance Act of 1968.[561] The NFIP, as implemented, is not an actuarially sound program. This is because the amount FEMA collects in premiums fails to cover the full risk exposure of the program. Over its history, the program has experienced years in which the amount generated by policy premiums was sufficient to cover claims. But the damages caused by Hurricanes Katrina and Rita in 2005 far exceeded program funding, meaning that FEMA had to borrow additional funding from the Treasury in order to cover losses.[562] The $16.3 billion in damage claims caused by Hurricane Katrina in the Gulf Coast region was more than all of the previous NFIP claims from significant flood events combined.[563] As of November 2012, FEMA owed the Treasury $20 billion, and had not repaid any principal on its loans since 2012.[564]

One of the reasons that the National Flood Insurance Programs is unsound and unable to cover its costs is the program's heavily subsidized premium rates. Under the program, there are two classes of premium rates, full-risk or actuarial rates, and subsidized rates. Actuarial rates are based on consideration of the risk involved and accepted actuarial principles.[565] Subsidized rates are set at a level that "would be reasonable, would encourage prospective insured to purchase flood insurance and would be consistent with the purposes of the legislation."[566] According to FEMA, about 22 percent of all NFIP policies are covered by subsidized rates.[567] These subsidized policy holders were grandfathered in to the program, despite the significant potential for economic lost and burden for the federal government in the event of a low-probability but devastating flood. The rationale for allowing subsidized premiums was to permit structures that were built in these high-risk areas prior to the general implementation of the program, and subsequent flood-related building codes, to be covered by flood insurance at reasonable rates. At the same time, properties that experience repetitive flood losses, known as "severe repetitive loss properties," account for a disproportionately large percentage of flood insurance claims, meaning that FEMA, and federal taxpayers, are paying out claims on the same

[561] Congressional Research Service, "The National Flood Insurance Program: Status and Remaining Issues for Congress," R42850, February 6, 2013.
[562] U.S. Government Accountability Office, "High-Risk Series: An Update," GAO-13-283, Washington D.C. February 2013, pg.261, available at http://www.gao.gov/assets/660/652133.pdf
[563] Congressional Research Service, "The National Flood Insurance Program: Status and Remaining Issues for Congress," R42850, February 6, 2013, pg.6.
[564] U.S. Government Accountability Office, "High-Risk Series: An Update," GAO-13-283, Washington D.C. February 2013, pg.261, available at http://www.gao.gov/assets/660/652133.pdf
[565] 42 U.S. Code § 2014 (a) (1).
[566] 42 U.S. Code § 2014 (a) (2).
[567] Congressional Research Service, "The National Flood Insurance Program: Status and Remaining Issues for Congress," R42850, February 6, 2013, pg. 19.

properties over and over again.[568] According to FEMA, these types of properties cost the program $12.1 billion as of December 2011.[569]

Policyholders receiving subsidized insurance rates through NFIP are getting a very good deal compared to what they would otherwise pay if they were required to insure the full cost of the risk exposure of their property. According to estimates, premiums for subsidized structures represent about 40 percent of the true risk premium,[570] at a projected average annual subsidized premium of $1,121 as of October 2010, discounted from the $2,500 to $2,800 that FEMA said would be required to cover the full risk of loss.[571] For properties in areas where the probability of flooding is particularly high, full-risk premium would cost triple the subsidized rates.[572]

In 2012, Congress took action to reform the unsustainable fiscal position of the NFIP and passed the Biggert-Waters Flood Insurance Reform Act, which included provisions that would raise premium rates, and reduce incentives to build in high-risk flood zones.[573] In particular, the law eliminated subsidies for second properties, required the phase-in of actuarial rates, and increased the annual cap on rate increases from 10 percent to 20 percent, among other provisions aimed at reforming program management.[574] Although the bill was not perfect, the GAO estimated that Biggert-Waters eliminated subsidies on roughly 438,000 policies, a key move to bring long overdue fiscal stability to the program and reduce taxpayers' exposure to flooding risks.[575]

But shifting some of the burden from taxpayers and the government to the owners of properties that are exposed to the risk of floods proved unpopular, particularly to the people who were facing higher premium costs. As is often the case in Congress, parochial interests trumped fiscally responsible reforms, and many of the changes made under Biggert-Waters were

---

[568] Congressional Research Service, "The National Flood Insurance Program: Status and Remaining Issues for Congress," R42850, February 6, 2013, pg. 20.
[569] Ibid, pg. 20.
[570] Federal Emergency Management Agency, "National Flood Insurance Program Actuarial Rate Review In Support of the Recommended October 1, 2011 Rate and Rule Changes," pg.9, available at https://www.fema.gov/media-library/assets/documents/23143?id=4853
[571] U.S. Government Accountability Office, "Flood Insurance: Public Policy Goals Provide a Framework for Reform," GAO-11-429T, March 11, 2011, pg. 4, available at http://www.gao.gov/assets/130/125706.pdf .
[572] Ibid, pg.5.
[573] Congressional Research Service, "The National Flood Insurance Program: Status and Remaining Issues for Congress," R42850, February 6, 2013, pg. 35.
[574] Ibid, pg. 35.
[575] U.S. Government Accountability Office, "Flood Insurance: More Information Needed on Subsidized Properties," GAO-13-607, July 2013, pg.12, available at http://www.gao.gov/assets/660/655734.pdf .

rolled back two years later by the Homeowner Flood Insurance Affordability Act of 2014.[576] This legislation required that refunds be paid to some policy holders who experienced rate increases under Biggert-Waters, limited the annual cap on premium rate increases to 18 percent, and removed the inclusion of catastrophic loss years (i.e. years like 2005 with Hurricane Katrina and Rita, or 2012 with Hurricane Sandy where losses are far higher than average years) from the average amount of obligations used to calculate how high premium rates must be to support the program.[577] Although supporters of this roll-back argued that it was necessary to protect homeowners and small businesses from the rate increases required by Biggert-Waters, the fact remains that many of the policies that actually benefit from outdated premium rates and unfair subsidies are located in places with higher home values and income levels.[578]

Put simply, after an all-too-rare attempt at legitimate reforms under the Biggert-Waters Act, Congress has once again left FEMA and the American taxpayers on the hook for billions of dollars in subsidized flood insurance premiums and claims payouts to rebuild homes and businesses that will continue to be located in high-risk flood zones that are better left to nature.

FEMA's Mitigation Programs

Another area of FEMA's work that should be a focus of additional oversight and evaluation is its programs for hazard mitigation.[579] The Department has several initiatives that are aimed to provide funding to states and localities to assist with mitigation measures in order to prevent or minimize the damage of future disasters. These programs include the Pre-Disaster Mitigation Program, the Hazard Mitigation Grant Program, and three mitigation programs related to the flood insurance program.[580]

---

[576] "Homeowner Flood Insurance Affordability Act," FEMA, at: http://www.fema.gov/media-library-data/1396551935597-4048b68f6d695a6eb6e6e7118d3ce464/HFIAA_Overview_FINAL_03282014.pdf, accessed December 31, 2014.
[577] Congressional Research Service, Bill Summary of H.R. 3370, available at https://www.congress.gov/bill/113th-congress/house-bill/3370 .
[578] Statement of Senator Mary Landrieu before the Subcommittee on Economic Policy, Committee on Banking, Housing and Urban Affairs Hearing "Implementation of the Biggert-Waters Flood Insurance Act of 2012: One Year After Enactment," Wednesday, September 18, 2013, pg.8, available at http://www.landrieu.senate.gov/files/documents/2013_09_18_landrieu_testimony.pdf and U.S. Government Accountability Office, "Flood Insurance: More Information Needed on Subsidized Properties," GAO-13-607, July 2013, pg.12 available at http://www.gao.gov/assets/660/655734.pdf .
[579] "What is Mitigation?," FEMA, at: https://www.fema.gov/what-mitigation, accessed December 31, 2014.
[580] Ibid.

Taxpayers have spent considerable resources on these programs and mitigation projects. According to the Congressional Research Service, the federal government has spent more than $11.4 billion on the Hazard Mitigation Grant Program between 1989 and 2014, and $7.8 billion of that was spent since 2003.[581] CRS also estimated that, since 2003, $3.4 billion in public assistance funds awarded have been spent on mitigation projects.[582]

Supporters of FEMA's mitigation spending and programs point to a 2005 FEMA-commissioned study which evaluated whether mitigation activities decrease future expenditures, and found that a dollar spent on mitigation results in four dollars saved in disaster spending.[583] However, Congress, the Department, and other watchdogs should study whether spending on mitigation projects have in fact yielded savings after FEMA has spent billions on these projects. For example, if spending on mitigation activities were indeed making the nation significantly more prepared for disasters and yielding significant savings, Congress should consider why states, localities, and private citizens are not prioritizing spending on these projects, and instead are reliant on the federal government to pay for these projects.

Congress should reconsider whether FEMA's spending on mitigation programs is necessary, effective, or even duplicative of other federal initiatives. At the very least, it should end the Pre-Disaster Mitigation Program. The current administration has proposed eliminating funding for the Pre-Disaster Mitigation Program, pointing to the existence of other mitigation spending within DHS, according to the Congressional Research Service.[584] The Administration also created a new competitive grant program for mitigation projects within the Department of Housing and Urban Development, raising the question of whether FEMA's programs are duplicative of other efforts.[585]

---

[581] Fran McCarthy, "FEMA Mitigation Spending," Congressional Research Service, Memorandum to the Senate Homeland Security and Governmental Affairs Committee, December 18, 2014.
[582] Ibid.
[583] "Natural Hazard Mitigation Saves: An Independent Study to Assess the Future Savings from Mitigation Activities. Volume 1 – Findings, Conclusions, and Recommendations," Multihazard Mitigation Council, National Institute of Building Science, 2005.
[584] Francis X. McCarthy, "FEMA's Pre-Disaster Mitigation Program: Overview and Issues," Congressional Research Service, August 27, 2014.
[585] Ibid.

Conclusion

While DHS's strategy states that it is working to make the nation more resilient, in reality the Department's programs exist largely to subsidized state and local emergency management, and effectively provide insurance for the public and private sector for disasters or other weather events. Moreover, it is not clear that DHS's spending on mitigation is doing much to make us safer when disasters actually occur. Thankfully, the agency has made much needed improvements to its immediate response activities when the big storms occur and when emergency assistance to save lives is urgently needed. Yet this is just a fraction of what FEMA actually does. FEMA's inability to make sound decisions when choosing what to pay to rebuild after disasters is costing taxpayers millions of dollars on a project-by-project basis, with no end in sight unless Congress or the agency fixes longstanding issues.

But the problem's related to DHS's and FEMA's programs are not their responsibility alone. The Department's programs for FEMA demonstrate Congress's priorities—encouraging agencies to deliver big subsidies to states, locals, and private owners (in the case of the National Flood Insurance Program) in order to drive the money back "home," rather than protecting taxpayers, and requiring DHS to focus on real, catastrophic national emergencies when federal assistance is urgently needed.

Other Key DHS Components, Directorates, Offices, and Programs

A review of DHS's mission and programs would be incomplete without assessing other key components, offices, directorates, and programs. The Department is the result of the largest reorganization of government since 1947 and, therefore, has other programs that are not directly tied to its five key mission areas. Assessing the reviews of these components, directorates, offices, and program areas is intended to help Congress and DHS leaders consider how to improve the Department's performance, efficiency, and ability to accomplish its missions.

The U.S. Coast Guard

The history of the U.S. Coast Guard (USCG) dates back to 1790, when a maritime law enforcement entity was established within the new Treasury Department to collect customs duties.[586] Today, the U.S. Coast Guard's mission is to be "the lead Federal agency for law enforcement, incident response, homeland security and disaster management in the maritime environment."[587]

On September 11, 2001, the U.S. Coast Guard led a water evacuation of more than half a million people from Manhattan, which former USCG Admiral James Loy called "bigger than Dunkirk," referring to the evacuation of Allied forces in the French port city in 1940.[588] The U.S. Coast Guard also mobilized to defend the nation's ports from a potential terrorist plot following the terrorist attacks.[589] Those attacks also marked the beginning of a new era for the U.S. Coast Guard, which included its transfer out of the Department of Transportation and into the new Department of Homeland Security.

As Congress and the Department consider options for reforming DHS, the U.S. Coast Guard is one of its biggest assets: A large component with a strong culture and effective management structure based on a clear chain of command. The USCG employs more than 42,190 active duty military personnel, 7,899 military reserves, as well as 8,700 civilians and

[586] U.S. Coast Guard, "Coast Guard Publication 1: Doctrine for the U.S. Coast Guard," February 2014, p.1.
[587] United States Coast Guard Snapshot, 2012, at http://www.uscg.mil/top/about/doc/uscg_snapshot.pdf, accessed November 7, 2014.
[588] Sam LaGrone, "Coast Guard Led 9-11 Water Evacuation Was 'Bigger Than Dunkirk," U.S. Naval Institute, July 23, 2014.
[589] Ibid.

32,156 auxiliary personnel.[590] The USCG maintains 244 cutters (commissioned vessels), 1,776 boats, and 198 aircraft.[591]

But how the USCG should best fit into DHS remains an open question, given the Coast Guard's extensive, varying missions and global responsibilities that extend far beyond protecting the homeland.[592] The USCG is the only military organization within DHS.[593] For example, the Coast Guard was mobilized during Operation Iraqi Freedom.[594] In fact, the U.S. Coast Guard does not devote most or even a majority of its time or resources to its homeland security mission. According to the DHS Inspector General's review of the U.S. Coast Guard's mission performance for FY 2013, the USCG dedicated about the same percentage of resource hours to homeland security missions as to non-homeland security missions.[595] DHS and the U.S. Coast Guard face a basic challenge of determining how to prioritize missions, including balancing its homeland security and non-homeland security missions. This challenge is compounded by U.S. Coast Guard's aging assets and its diverse and increasing responsibilities.

Reviewing the USCG's Missions and Ability to Execute Them

The U.S. Coast Guard is an example of how Congress creates problematic requirements for DHS and its components; including requiring it to have a broad mission that may not be realistic for it to accomplish given its resources. In a 2014 review of the U.S. Coast Guard's mission, the Office of Inspector General explained that the Homeland Security Act of 2002 "prohibits the Secretary of Homeland Security from substantially reducing any of the U.S. Coast Guard's missions after its transfer to the Department of Homeland Security, except as specified in subsequent acts."[596] Congress and DHS should conduct a thorough review of the USCG's

[590] United States Coast Guard Snapshot, 2012.
[591] Ibid.
[592] Section 888 of the Homeland Security Act of 2002, Public Law 107-296, defines the USCG's 11 statutory missions as either non-homeland security missions or homeland security missions. There are 6 non-homeland security missions and 5 homeland security missions. DHS Office of Inspector General, Annual Review of the U.S. Coast Guard's Mission Performance (FY2013)," OIG-14-140, September 11, 2014, p.5.
[593] "DHS Components," Department of Homeland Security, at: http://www.dhs.gov/department-components, accessed December 29, 2014.
[594] Basil Tripsas, Patrick Roth, Renee Fye, "Coast Guard Operations During Operation Iraqi Freedom," CNA, October 2004.
[595] DHS Office of Inspector General, Annual Review of the U.S. Coast Guard's Mission Performance (FY2013)," OIG-14-140, September 11, 2014
[596] The Inspector General reports that the USCG was more successful meeting its non-homeland security performance measures, including meeting 9 out of 12 targets. "Annual Review of the U.S. Coast Guard's Mission

missions and their relevance to the overall strategy of homeland security, prioritizing its missions and identifying those that are non-essential or could be better performed by other agencies. The status quo results in DHS and the U.S. Coast Guard not successfully executing all of its missions. The Inspector General reported that the USCG did not meet 8 of its 23 performance measures, including missing its targets on 5 out of 11 homeland security measures.[597]

The U.S. Coast Guard, on its website[598], list its missions in the following order based on the percentage of operating expenses allocated to each area:

1. "Ports, waterways, and coastal security"
2. "Drug interdiction"
3. "Aids to navigation"
4. "Search and rescue"
5. "Living marine resources"
6. "Marine safety"
7. "Defense readiness"
8. "Migrant interdiction"
9. "Marine environmental protection"
10. "Ice operations"
11. "Other law enforcement" [599]

Some of these operations are clearly linked to homeland security and DHS's overarching missions of preventing terrorism and securing the nation's ports and maritime environment. The U.S. Coast Guard continues to play a lead role in Operation Noble Eagle, the national security operation to secure the homeland that began days after September 11, 2001.[600] However, other USCG missions extend far beyond homeland security, such as providing icebreaker services for the polar region[601] and collaborating with other federal agencies, such as the National Science Foundation for ice breaking used to enable scientific research.[602] The Coast Guard also plays

---

Performance (FY2013)," DHS Office of Inspector General, September 2014, http://www.oig.dhs.gov/assets/Mgmt/2014/OIG_14-140_Sep14.pdf, accessed November 7, 2014.
[597] Ibid.
[598] U.S. Coast Guard, "Missions," at: http://www.uscg.mil/top/missions/, accessed December 23, 2014.
[599] Ibid.
[600] "The Coast Guard & Homeland Security," U.S. Coast Guard, U.S. Department of Homeland Security, at http://www.uscg.mil/history/uscghist/Homeland_Security.asp, accessed December 29, 2014.
[601] "Report to Congress: U.S. Coast Guard Polar Operations," U.S. Coast Guard, FY2008, at: http://www.uscg.mil/history/ops/ice/docs/FY08_OMNIBUS_Polar_Ops.pdf, accessed December 29, 2014.
[602] "Mobility and Ice Operations Division," U.S. Coast Guard, U.S. Department of Homeland Security, at: http://www.uscg.mil/hq/cg5/cg552/ice.asp, accessed December 29, 2014.

the lead and coordinator role for oil spills of national significance, such as in the case of the 2010 Deepwater Horizon oil spill in the Gulf of Mexico.[603]

An Aging Fleet and Assets

Another challenge for the USCG is the effect of aging assets on the Coast Guard's ability to perform its missions. As the Government Accountability Office reported in 2012, many of the USCG's assets are approaching the end of their planned service lives, including some vessels that were created more than thirty or forty years ago.[604] The aging fleet creates costs for the Coast Guard, including maintenance and upkeep, and also limits the USCG's operational capabilities.[605] For example, GAO's review of the state of the Coast Guards fleet found that many of their vessels operate for much of the time with significant problems.[606]

But DHS and the Coast Guard have struggled to effectively replace its fleet. GAO reported that the Coast Guard's long-term capitalization project has experienced cost and management problems, which have led to significant delays in the delivery of new vessels, including some by up to 13 years.[607] The Congressional Research Service noted concerns about the adequacy of information available to Congress to "support review and oversight of Coast Guard procurement programs, including cutter procurement programs."[608]

The Coast Guard's icebreaker fleet is emblematic of the USCG's recapitalization challenges. For example, in 2011, the Inspector General warned that the USCG "does not have the necessary budgetary control over its icebreakers, nor does it have a sufficient number of icebreakers to accomplish its mission in the Polar Regions," which are required by statute and

[603] Josh Hicks, "IG: Coast Guard falling short on Deepwater Horizon recommendations," Washington Post, March 11, 2014.
[604] Government Accountability Office, Coast Guard [:] Mission Performance Challenged by the Declining Condition and Rising Costs of its Legacy Vessel Fleet, GAO-12-934T, September 20, 2012. Testimony given before the Subcommittee on Coast Guard and Maritime Transportation, Committee on Transportation and Infrastructure.
[605] Ibid. GAO reported that USCG's asserts operated with significant casualties for much of the time: 56 percent of the time for high endurance cutters, 35 percent of for medium endurance cutters, and 28 percent for patrol boats, below the USCG's operational targets.
[606] Ibid, p.3. GAO reported that: over a seven year period, Coast Guard's vessels operated with major casualties for much of their operational time: 6 percent of the time for high endurance cutters, 35 percent of for medium endurance cutters, and 28 percent for patrol boats, below the USCG's operational targets.
[607] Ibid.
[608] Congressional Research Service Memorandum, Coast Guard Cutter Procurement: Background and Issues for Congress, by Ronald O'Rourke, April 9, 2014, pp. 31-33.

presidential directives.[609] The report goes on to note that "should the Coast Guard not obtain funding for new icebreakers or major service life extensions for its existing icebreakers with sufficient lead-time, the United States will have no heavy icebreaking capability beyond 2020 and no polar icebreaking capability of any kind by 2029."[610] As of 2014, the U.S. Coast Guard has two icebreakers, the Polar Star for breaking heavy ice and the Healy, a medium icebreaker, which is primarily capable of supporting scientific research, according to the Congressional Research Service.[611] The U.S. Coast Guard is considering options for replacing the Polar Star when it reaches the end of its service life by 2022, including building a new icebreaker or reactivating the Polar Sea, which went inactive after engine failure in 2010.[612]

USCG's Challenges with Information Technology Projects

Along with its challenges with fleet recapitalization, the U.S. Coast Guard has also struggled with some key information technology initiatives that were aimed to support and harmonize decision-making and operations across the USCG's vast areas of responsibility, as well as share information with key partners. For example, the Coast Guard's initiative to create a Common Operational Picture and share information between its assets and commanders is still not successfully deployed across the USCG. Several recent GAO audits have identified these struggles, despite the large expenditures that have been made on these information technology projects. In 2011, GAO reported that the Coast Guard had "not met its goal of building a single, fully operational Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance program (C4ISR) system," despite spending $2.5 billion.[613] A February 2012 audit found that USCG's Watchkeeper software, a key component of a $74 million project to collect and share information for operators involved with port security, "met few port agency partner needs, in part because the agency failed to determine these needs

[609] Department of Homeland Security Office of Inspector General, "The Coast Guard's Polar Icebreaker Maintenance, Upgrade, and Acquisition Program," OIG-11-31, January 2011.
[610] Department of Homeland Security Office of Inspector General, The Coast Guard's Polar Icebreaker Maintenance, Upgrade, and Acquisition Program, OIG-11-31, January 2011, pp. 1 (Executive Summary) and 10.
[611] Ronald O'Rourke, "Coast Guard Polar Icebreaker Modernization: Background and Issues for Congress," Congressional Research Service, August 4, 2014.
[612] Ibid.
[613] Government Accountability Office, Coast Guard: Observations on Progress Made and Challenges Faced in Developing and Implementing a Common Operational Picture, GAO-13- 784T, July 31, 2013, p. 2.

when developing the system."[614] Overall, GAO reported in 2013 that the Coast Guard had failed to follow "its own information technology acquisitions guidance and processes" for several initiatives which resulted in "poor usability and the inability to share information as intended."[615]

A 2014 DHS Inspector General audit of DHS's information technology modernization project found that, while USCG has "implemented information technology systems that effectively support the mission needs of some ships and aircraft," other "ships and aircraft continue to rely on obsolete technology which impacts mission performance and makes operations and maintenance more difficult and costly."[616] The Inspector General pointed to "significant budgetary reductions" as one reason why information technology improvements were not made.[617] While resources may be a problem, improving its information technology acquisition and deployment initiatives should be a priority for the Coast Guard, and an area of ongoing focus and oversight for Congress.

Considering the Future of the U.S. Coast Guard

Congress has a responsibility to review and reconsider the U.S. Coast Guard to determine what is an achievable mission, and the realistic level of resources that is necessary to successfully accomplish it. "There is no way to predict the next major crisis, but our operating environment is profoundly harsh and unforgiving," explained Commandant Paul F. Zukunft at his confirmation hearing in 2014. Absent reform, the U.S. Coast Guard will face a challenge of trying to balance broad responsibilities without the required resources to successfully achieve each mission.

As a military organization, the Coast Guard is the component within DHS that has the strongest culture and most effective management. Congress and the Department of Homeland Security could consider shifting additional resources and responsibilities from other DHS components and offices into the Coast Guard. For example, Secretary Jeh Johnson's choice to put the Coast Guard in charge of developing a department-wide strategy and campaign plans for

[614] Ibid.
[615] Ibid, p.7.
[616] "U.S. Coast Guard Command, Control, Communication, Computers, Intelligence, Surveillance, and Reconnaissance Modernization," DHS OIG, October 28, 2014, http://www.oig.dhs.gov/assets/Mgmt/2015/OIG_15-05_Oct14.pdf, accessed on November 7, 2014.
[617] Ibid.

securing the southern border raises an interesting question of whether USCG could be a more effective entity for securing the border than Customs and Border Protection if given sufficient resources. However, a significant shift in resources and responsibilities is unlikely unless Congress were to undertake a comprehensive reorganization of DHS.

The basic questions that Congress and the Department should ask are what the Coast Guard's mission should be, and what resources are needed to achieve it. While DHS is prohibited from refocusing USCG's missions,[618] Congress should work to realign the Coast Guard and its missions so that most of its resources are allocated to the homeland security mission set, and allow the Coast Guard to scale back on its non-security responsibilities.

[618] Section 888 of the Homeland Security Act of 2002, Public Law 107-296.

The Office of Health Affairs

According to the 2014 Quadrennial Homeland Security Review (QHSR), "Of the naturally occurring events, a devastating pandemic remains the highest homeland security risk."[619] The QHSR further warned, "Both the likelihood and consequences of this low probability, high-impact event are expected to increase, driven in large part by increasing opportunities for novel infectious diseases to emerge and spread quickly around the world."[620]

The American public became acutely aware of the horrific potential of a low-probability, high-impact pandemic or serious health threat during the 2014 outbreak of Ebola in West Africa, and the arrival of the disease in the United States. While the domestic outbreak has been minimal to date and was contained, it raised a legitimate question of whether the nation is prepared for a devastating pandemic.

Responsibilities for addressing a pandemic and other health risks are assigned to several agencies across the federal government, including the Department of Health and Human Services Department (HHS) and Centers for Disease Control and Prevention (CDC). One of the Department of Homeland Security's roles is supporting "efforts to develop and execute pandemic contingency plans and preparedness actions as part of the United States Government's pandemic preparedness strategy."[621] This role stems in part from Homeland Security Presidential Directive 8 and the National Response Framework, which designate the Secretary of Homeland Security as the coordinator of domestic emergency response. Despite its responsibilities related to pandemics, DHS has only one pandemic plan, for pandemic influenza, and has not updated it since September 2006.[622] DHS's apparent lack of preparedness or pandemics and other health security risks is alarming given the Department's own position made clear in the QHSR that pandemics present the greatest of all threats to homeland security.

---

[619] The 2014 Quadrennial Homeland Security Review, U.S. Department of Homeland Security, p.21.
[620] Id.
[621] DHS Office of Inspector General, "DHS Has Not Effectively Managed Pandemic Personal Protective Equipment and Antiviral Medical Countermeasures," OIG-14-129, August 2014.
[622] "Pandemic Influenza Preparedness, Response, and Recovery: Guide for Critical Infrastructure and Key Resources," September 2006, at http://www.flu.gov/planning-preparedness/business/cikrpandemicinfluenzaguide.pdf, accessed November 7, 2014.

The Office of Health Affairs (OHA), which received $127 million in appropriations for FY 2014,[623] is the lead office within DHS for health issues, including pandemics, workforce health protection, medical oversight, and chemical and biological defenses.[624] In the event of a pandemic, DHS would need to ensure both that its workforce had the resources and ability to continue critical operations, and also support other governmental efforts to address public health and public safety needs.

In September 2014, the Inspector General released an audit of DHS's management of pandemic preparedness resources, including personal protective equipment and antiviral medications, and the use of $47 million in funds appropriated to DHS in 2006 for planning, training, and preparing for a potential pandemic.[625] The Inspector General recently testified to the House Committee on Oversight and Government Reform about what was learned: "In short, our audit concluded that DHS did not adequately assess its needs before purchasing pandemic preparedness supplies and then did not adequately manage the supplies it had purchased."[626]

The specifics of the audit, which the Inspector General described in his House testimony, show examples of poor planning, mismanagement, and how these problems lead to waste. Further, that these problems could hinder the Department's ability to operate and execute its responsibilities in the event of a pandemic.[627] For example, DHS acquired a stockpile of 350,000 protective suits for personnel in the National Capital Region as well as 16 million surgical masks, but did not have justifications for why these resources were necessary.[628] The Department has on hand nearly 5,000 bottles of hand sanitizer, of which 84 percent were expired and in some cases, by up to 4 years.[629] The Inspector General also reported that DHS has also struggled to manage its stockpile of antiviral drugs which could be used in the event of a pandemic.[630] For example, DHS had to recall $600,000 worth of medications based on concerns

[623] William L. Painter, "Department of Homeland Security: FY2014 Appropriations," Congressional Research Service, April 18, 2014.
[624] The Office of Health Affairs describes itself as the "principal authority for all medical and health issues" on its website. "Overview," Office of Health Affairs, U.S. Department of Homeland Security, at: http://www.dhs.gov/office-health-affairs, accessed December 29, 2014.
[625] DHS Office of Inspector General, "DHS Has Not Effectively Managed Pandemic Personal Protective Equipment and Antiviral Medical Countermeasures," OIG-14-129, August 2014.
[626] John Roth, Inspector General, Department of Homeland Security, Statement Before the Committee on Oversight and Government Reform, U.S. House of Representatives, October 24, 2014.
[627] Ibid.
[628] Ibid.
[629] Ibid.
[630] Ibid.

that they may be unsafe or ineffective, since the Inspector General had discovered that many of the drugs were stored improperly, raising questions about their continued potency.[631] The Inspector General also questioned the usability of $5 million in medical countermeasure drugs that CBP was managing due to uncertainty about storage conditions.[632] The OIG determined that TSA has a stock of 200,000 respirators, which have exceeded the manufacturer's 5-year usability guarantee.[633]

The Department recognized the importance of addressing problems in its pandemic preparedness work, and has agreed to take steps to address the problems identified by the Inspector General's audit.[634] The apparent lack of planning, and mismanagement of past resources to address or mitigate potential health risks, raises serious questions about whether DHS is ready to execute its responsibilities, including protecting its workers, in the event of a serious threat to the nation's health security.

During the recent scare related to the outbreak of Ebola in West Africa, and arrival of the disease in the United States, minority staff spoke with representatives of several unions that represent frontline workers. The representatives for the U.S. Border Patrol's union[635] and U.S. Citizenship and Immigration Service employees[636] reported that their members had not received training or adequate personal protective equipment to ensure that they could take appropriate precautions to protect themselves in the event of a severe Ebola outbreak in the United States. Fortunately, Customs and Border Protection officers at ports of entry, who are likely at the greatest risk of exposure to a potential health risk traveling into the country, had received training and protective measures, according to their union representative.[637]

Given the serious consequences associated with a pandemic, as well as other health security risks, DHS's Office of Health Affairs should be a focus of oversight and attention both for the Department and the Congress moving forward. As discussed in an earlier section, the

---

[631] Ibid.
[632] Ibid.
[633] Ibid.
[634] DHS agreed with and plans to implement all of the Inspector General's recommendations for improving pandemic preparedness planning and resource management. DHS Office of Inspector General, "DHS Has Not Effectively Managed Pandemic Personal Protective Equipment and Antiviral Medical Countermeasures," OIG-14-129, August 2014.
[635] Email from the representative of the Border Patrol Agent Union to minority committee staff, October 15, 2014.
[636] Email from the representative of the National Citizenship and Immigration Services Council to minority committee staff, October 14, 2014.
[637] Email from representative of the National Treasury Employees Union (which represents CBO officers) to minority committee staff, October 15, 2014.

Department has struggled with other initiatives that fall under OHA's responsibility, including developing and deploying effective bio-surveillance technologies and systems to protect against potential biological threats, like BioWatch.[638] That OHA and the Department are struggling with executing its pandemic preparedness responsibilities raises further questions and concern about whether the Department is executing its mission related to threats to health security.

Science and Technology (S&T) Directorate

The S&T Directorate is DHS's primary arm for research and development (R&D). This includes conducting R&D for other components, and coordinating all R&D across the Department.[639] According to the Department's authorizing act, one of the original purposes of DHS's S&T Directorate was: "conducting basic and applied research, development, testing and evaluation … [and] coordinating and integrating all research, development, testing and evaluation activities of the Department."[640] The primary purpose of DHS's Science and Technology (S&T) Directorate can largely be divided into two areas: research and development, and acquisitions support.[641] Each of the S&T Directorate's divisions and offices can be traced back to one or both of these functions.[642] The Directorate's R&D function is divided further into two subsets of R&D: R&D for state and local first responders (for example, advanced structural gloves for firefighters) and R&D for the DHS components (for example, tunnel detection systems for U.S. Customs and Border Patrol). Acquisitions support is largely a

[638] GAO, "Observations on the Cancelation of BioWatch Gen-3 and Future Considerations of the Program," GAO-14-267T, June 10, 2014.
[639] 6 U.S.C. 182 (2012).
[640] Homeland Security Act of 2002, Pub. L. 107-296, § 302, 116 Stat. 2135, 2163-64 (codified as amended at 6 U.S.C. § 182). In a hearing on the authorizing act, Representative Boehlert made plain the Directorate's important envisioned role in R&D oversight at the Department: "The Science Committee felt, as did several other Committees, that HR 5005 did not pay adequate attention to R&D. The bill did not spell out the R&D responsibilities or activities of the new Department, did not give them a central focus, and did not designate a senior official who would be accountable for - or for that matter, have the background to run - the Department's R&D programs. We thought that was a recipe for failure, and we can't afford failure in this area. … So, following the recommendations of the National Academy of Sciences, among others, we created an Under Secretary for Science and Technology and gave that person clear responsibilities for R&D across the Department." Hearing on H.R. 5005, The Homeland Security Act of 2002Before the H. Select Comm. on Homeland Sec., 107th Cong. (2002). (Statement of Rep. Sherwood Boehlert, Chairman, House Committee on Science).
[641] Science and Technology Directorate Organization Chart, U.S. Department of Homeland Security, at: https://www.dhs.gov/sites/default/files/publications/Visio-ST%20Org%20Chart%20-%202.pdf, accessed December 29, 2014.
[642] Id.

function of providing expertise on specific acquisitions, developing standards, and coordination of testing and evaluation.[643]

While DHS's Science and Technology Directorate has made progress in recent years, and has had capable leadership in former Under Secretary Dr. Tara O'Toole and current Under Secretary Dr. Reginald Brothers, there are many open questions about the S&T Directorate's work and effectiveness. Specifically, it remains unclear how effectively DHS is coordinating research and development across the department, whether S&T is significantly improving the homeland security mission of DHS and its partners, and whether S&T provides useful acquisition support. In some cases, S&T's research and development projects may be unnecessary or duplicative of other government or private sector research. The S&T Directorate and the Department's research and development initiatives are areas that are ripe for additional oversight and review. Ultimately, the Department and Congress must review S&T's work and responsibilities, and reconsider whether a Department-wide reorganization of DHS research and development would be beneficial and whether DHS's R&D mission can be refocused and reprioritized to yield more value for the nation's security.

DHS Has Struggled with Department-Wide Coordination of Research and Development

DHS and the Science and Technology (S&T) Directorate have struggled to set a unified definition for research and development across the Department, and thus DHS cannot track how much it is spending on R&D.[644] The only DHS components other than the S&T Directorate with statutory authority to conduct R&D within the Department are the Coast Guard and the Domestic Nuclear Detection Office.[645] Nevertheless, due to the lack of a Department-wide definition of research and development, a number of other components participate in activities that are fairly described as R&D. In a 2012 report, the Government Accountability Office found that as a result of the lack of a single Department-wide definition of R&D, there was a potential for duplication.[646] GAO reported that seven other DHS components engaged in at least $255

[643] Id.
[644] Statement of David C. Mauer, Government Accountability Office, "Department of Homeland Security: Actions Needed to Strengthen Management of Research and Development," GAO-14-865T, September 9, 2014.
[645] Dana Shea and Daniel Morgan, "The DHS Directorate of Science and Technology: Key Issues for Congress," Congressional Research Service, June 22, 2009.
[646] Government Accountability Office, "Department of Homeland Security: Oversight and Coordination of Research and Development Should Be Strengthened, GAO-12-837, September 2012.

million in R&D work that went unreported to OMB, and was not coordinated by S&T; raising concerns that there may have been duplication between those components' work and other public and private sector research.[647] GAO recommended that the Secretary identify a Department-wide definition of R&D to avoid the potential for duplication. According to the S&T Directorate's 2014 Review, the Directorate has proposed a definition of R&D for the Department, but it has yet to be approved.[648]

The lack of transparency in the Department's management of R&D spending creates a risk of inefficiency. In order to select R&D projects that will be the most useful to DHS components, S&T prioritizes those projects that receive "customer funding" or in-kind support from those components. In other words, part of S&T's R&D budget for its R&D activities comes from reimbursements from other components. This model is helpful in reducing the number of projects that will never succeed or will not be useful to operational components at DHS, since operational components willingness to share in the cost of a project show their belief in its potential utility and are more likely to convince S&T to engage on the project. However, it also reduces transparency of R&D spending department-wide, transparency of S&T's budget, and transparency of spending on specific projects because in-kind support and outlays are not reported to OMB, nor are they part of the S&T budget request made to Congress.[649]

The Effectiveness of DHS's R&D Spending Remains Unknown

Besides questions concerning the management and coordination of DHS's research and development projects, it remains unclear how much S&T and DHS's other R&D projects are improving the homeland security mission. The exact amount of R&D spending at DHS is unclear, though it likely exceeds $1 billion annually.[650] Former Secretary Napolitano has also

[647] Id.
[648] Id.
[649] Further complicating S&T's budget and reducing transparency into specific projects, in FY2012 S&T realigned its budget structure to place most of R&D activities into a single Project/Program/Activity (PPA), providing Congress with less insight into and control over the Directorate's R&D work than the previous budget structure, which aligned R&D with specific topic areas. Despite objections by both the Senate and House Appropriations Committees in 2012, the conference committee for the 2012 DHS Appropriations Act supported the realignment and the practice continues to date. H. Rept. 112-331, p. 998; CRS R43064.
[650] See John F. Sargent, Jr., Federal Research and Development Funding: FY2013, Congressional Research Service, R42410, p. 19. CRS's analysis showed $1.122 billion in DHS R&D budgetary authority for S&T, DNDO, and the Coast Guard for FY 2011 and $984 million for FY 2012.; Government Accountability Office, Department of Homeland Security: Oversight and Coordination of Research and Development Should be Strengthened, GAO-12-

cited science and technology as a key tool and priority in achieving the Department's mission.[651] Yet the extent to which these R&D projects are making the nation safer remains unclear. For example, evidence suggests that S&T's own customers, including components within the Department, are unsatisfied with its work. For example, GAO interviewed representatives from those components to evaluate their impression of S&T's work, and their responses were not positive. According to GAO, those components surveyed consistently said they were aware of few or no products that S&T had transitioned from one of S&T's R&D projects to their respective components.[652]

The Department's struggles over the past twelve years with significant R&D and acquisitions projects, such as TSA's screening technologies and the various biological and nuclear detection tools which were reviewed earlier in this report, are well known. The minority staff reviewed a list of the S&T Directorate's current R&D projects as of July 2013, and determined that many of the projects are aimed at problems, which, if solved, could correct significant issues for homeland security or yield significant benefits for homeland security stakeholders. From improved equipment for fire fighters to technology to identify IEDs and/or potential biohazard incidents, many of S&T's current (in-house) research projects can be justified as aiming to solve a legitimate problem.

However, Congress and the Department must evaluate these expenditures to determine whether its R&D projects are truly federal or DHS responsibilities, as well as whether these projects may be duplicative of other federal research initiatives. For example, S&T is currently managing a slate of cyber security research and development projects. It is certainly possible that this research could be duplicating research efforts of other federal agencies and the private sector. To its credit, S&T has implemented an annual Portfolio Review that has at least halved the number of projects S&T is working on, and narrowed the scope of its R&D projects to ones that have a higher likelihood of success and faster transition time. However, S&T does not

---

837, September 2012, p. 10. GAO identified $255 million in R&D obligations in FY 2011 from components other than S&T, DNDO, and the Coast Guard that were not reported as R&D to OMB.

[651] Statement of Tara J. O'Toole, Hearing on the Nomination of Tara J. O'Toole to be Under Secretary for Science and Technology of the United States Department of Homeland Security Before the Senate Committee on Homeland Security and Governmental Affairs, March 3, 2010.

[652] Briefing by David Maurer, Director, Homeland Security and Justice, GAO, July 8, 2013.

appear to have a system in place to evaluate a project after completion—to determine its ongoing utility to the component or effectiveness in achieving its goal.[653]

Whether DHS's R&D projects are duplicative of or potentially subsidizing private sector research and development initiatives also remains an open question. For example, one of the components within DHS S&T is its First Responder Group (FRG), which "pursues a better understanding of the response community's needs… provides technical assistance, and develops innovative solutions to the most pressing challenges faced during…emergencies."[654] Through FRG, S&T partners with the private sector to fund the development of first responder technologies, such as lighter fire-retardant materials for firefighter gloves and turnout gear.[655] However, a number of private companies are also involved in R&D for first responders. For example, DuPont developed both Nomex®[656] and Kevlar® fabrics,[657] which are used by many firefighters and police officers. It is possible, therefore, that S&T's First Responder Group may duplicate or subsidize private sector research and innovation that may occur without DHS's help. S&T also has no cost-recovery mechanism that would allow it to recover costs spent on the technologies that it develops and are subsequently put to use by the private sector.[658] Instead, S&T provides its designs to manufacturers free of cost, and those manufactures are then free to profit off of DHS's taxpayer-funded R&D.

Some of the projects that the Science and Technology Directorate funds appear to be of little value to the nation's homeland security mission. For example, S&T funds research projects at nine-university based "Centers of Excellence," at a cost of more than $3 million annually. Altogether, the Directorate has spent at least $352 million on research centers at universities across the country. The results or benefits of these expenditures remain unclear. The following are some of the research studies that have been funded by the Department through the Centers of Excellence Program:

---

[653] Minority Staff Communications with S&T's Legislative Affairs office and GAO whether such a system is in place, but neither were aware of one.
[654] Science and Technology Directorate Support to the Homeland Security Enterprise and First Responders, Department of Homeland Security, at https://www.dhs.gov/st-frg, accessed July 13, 2013.
[655] Science and Technology Directorate, Department of Homeland Security, Improved Structural Firefighting Glove (2013); Science and Technology Directorate, Department of Homeland Security, Wildland Firefighter Advanced Personal Protection System (2013).
[656] Nomex® Brand, DuPont, at http://www.dupont.com/products-and-services/personal-protective-equipment/thermal-protective/brands/nomex.html, accessed July 13, 2013.
[657] Kevlar® Brand, DuPont, at http://www.dupont.com/products-and-services/fabrics-fibers-nonwovens/fibers/brands/kevlar.html, accessed July 13, 2013.
[658] Committee staff briefing with S&T budget officials on the President's FY 2014 proposed budget, April 11, 2013.

- "*Indigenous Knowledge and Sea Ice Science: What Can We Learn from Indigenous Ice Users*?" The University of Hawaii [659]

- "*Household Income, Poverty, and Food Stamp Use in Native-Born and Immigrant Households: A Case Study in Use of Public Assistance,*" The University of Arizona[660]

- "*Reasons for Secrecy and Deception in Homeland-Security Resource Allocation,*" University of Southern California[661]

These kinds of academic projects may have value to researchers and the academic community, but they do not appear to provide any meaningful benefit to the nation's security.

DHS's R&D Initiatives and Assets Should be Streamlined and Reorganized

The Department and Congress should consider and review options for streamlining and reorganizing DHS's approach to scientific research and development. For example, a former senior DHS official advocated for consolidating chemical, biological, radiological, and nuclear (CBRN) security responsibilities into a single directorate at DHS. The Department's CBRN security responsibilities are scattered across DHS's organization, and the current situation is disjointed, inefficient, and leads to a lack of competency and leadership within any single component. Currently, agencies with CBRN responsibilities at the Department include: FEMA, ICE, CBP, and NPPD, as well as R&D components like S&T, the Domestic Nuclear Detection Office (DNDO), and the Office of Health Affairs (OHA). Congress and the Department should consider consolidating all R&D functions into the Science and Technology Directorate or a new weapons of mass destruction (WMD) directorate focused on the CBRN threat, including DNDO's research on WMD and OHA's bio-surveillance responsibilities.

---

[659] Eiskeen, H, "Indigenous knowledge of sea ice science: What can we learn from indigenous ice users?, Center for Island, Maritime, and Extreme Environment Security, University of Hawaii, 2010, at: http://www.cimes.hawaii.edu/node/437, accessed December 30, 2014.

[660] Judith Gans, "*Household Income, Poverty, and Food Stamp Use in Native-Born and Immigrant Households: A Case Study in Use of Public Assistance,*" Udall Center for Studies in Public Policy, The University of Arizona, National Center for Border Security and Immigration, at: http://www.borders.arizona.edu/cms/sites/default/files/gans_2013a.pdf, accessed December 30, 2014.

[661] Jun Zhuang, Vicki M. Bier, "Reasons for Secrecy and Deception in Homeland Security Resource Allocation, CREATE Homeland Security Center, University of Southern California, at: http://research.create.usc.edu/published_papers/110/, accessed December 30, 2014.

The Construction of the NBAF Facility Requires Oversight and Effective Management

One major program the Directorate will oversee over the coming years is construction of the new National Bio and Agro Defense Facility in Manhattan, Kansas (NBAF), replacing the aging Plum Island Animal Disease Center (PIADC) in New York. The NBAF facility is intended to offer several benefits over the existing facility, including providing the highest biosecurity and biocontainment standard for a lab that can accommodate large animals. NBAF is slated to cost approximately $1.2 billion,[662] and scheduled to be completed and operational by 2023.[663] Given DHS's past challenges with complex acquisitions and constructions projects, including the construction of the St. Elizabeths campus (discussed later in this report), Congress and the Department should closely monitor the project in order to ensure that it is being completed on schedule and on budget.

The Office of Inspector General

The DHS Office of Inspector (OIG) currently receives approximately $140 million in annual funding,[664] and is comprised of 680 employees.[665] The tax dollars that Congress invests in the Inspector General's office are among the most important directed to the Department, since the OIG is the taxpayer's watchdog within DHS, assigned the statutory responsibility of investigating and auditing the Department's programs and workforce to identify criminality, waste, fraud, and abuse.[666]

The OIG can point to significant accomplishments. Each year, the OIG identifies areas where the Department can create cost savings, including by recovering or putting funds to better use, which exceed hundreds of millions in savings each year.[667] The OIG also produces

[662] The project includes approximately $300 million in matching funds from Kansas.
[663] "National Bio and Agro-Defense Facility," Science and Technology Directorate, Department of Homeland Security, at: http://www.dhs.gov/national-bio-and-agro-defense-facility, accessed December 30, 2014.
[664] DHS FY2014 Budget in Brief, p.6.
[665] Office of Inspector General, Department of Homeland Security, "Semiannual Report to the Congress, April 1, 2013 through September 30, 2013," at: http://www.oig.dhs.gov/assets/SAR/OIG_SAR_Apr13_Sep13.pdf.
[666] According to its website, "the OIG conducts and supervises independent audits, investigations, and inspections of the programs and operations of DHS, and recommends ways for DHS to carry out its responsibilities in the most effective, efficient, and economical manner possible. We also seek to deter, identify and address fraud, abuse, mismanagement, and waste of taxpayer funds invested in Homeland Security," see: DHS OIG, "What We Do," at: http://www.oig.dhs.gov/index.php?option=com_content&view=article&id=94:what-we-do&catid=2&Itemid=63 , accessed December 30, 2014.
[667] Office of Inspector General, Department of Homeland Security, "Semiannual Report to the Congress, April 1, 2013 through September 30, 2013."

reports and audits of DHS programs, identifying problems and offering recommendations to the Department and Congress. The OIG's collection of audits was one of the key bodies of available oversight work and evidence that was used for the analysis and judgments presented in this report. The Inspector General is also charged with the critical responsibility of investigating potential instances of criminality and other wrongdoing within the Department's workforce. For a six month period in 2013, for example, the Inspector General reported 1,011 open investigations, 197 investigations referred for prosecution, 56 investigations accepted for prosecution, 98 arrests, 71 indictments, 43 convictions, and 29 personnel actions.[668]

Past Problems Related to Independence and Integrity

Unfortunately, the DHS Office of Inspector General has suffered from serious questions about its own independence and the actions of some of its employees, including the OIG's Acting Inspector General before December 2013. The former Acting Inspector General, who was in the position from February 2011 until his resignation in December 2013, faced serious allegations of nepotism, abuse of power, misuse of government funds for personal use, and politicization. A bipartisan investigation conducted by Senator Claire McCaskill and Senator Ron Johnson, chair and ranking member of the Subcommittee on Financial and Contracting Oversight reached the following conclusion:

> …Mr. Edwards' inadequate understanding of the importance of OIG independence and his frequent communications and personal friendships with senior DHS officials. Mr. Edwards did not obtain independent legal advice and directed reports to be altered or delayed to accommodate senior DHS officials. Mr. Edwards also did not recuse himself from audits and inspections that had a conflict of interest related to his wife's employment.[669]

The findings of the investigation raised serious questions about the OIG's integrity, independence, and whether the OIG was fulfilling its oversight responsibilities of the Department's workforce and programs. The issues of politicization[670] and questions about independence were particularly troubling.[671]

---

[668] Ibid, p.2.
[669] "Investigation into Allegations of Misconduct by the Former Acting and Deputy Inspector General of the Department of Homeland Security," Staff Report, Subcommittee on Financial and Contracting Oversight, Committee on Homeland Security and Governmental Affairs, United States Senate, April 24, 2014.
[670] According to the FCO subcommittee report, issues of politicization under the former acting Inspector General's leadership were frequently brought forward by internal whistleblowers. The former acting Inspector General

In March 2014, John Roth was confirmed as the new Inspector General, earning widespread bipartisan support for his nomination in the U.S. Senate. Mr. Roth's nomination and confirmation was an opportunity for the entire Office of Inspector General to create a new era, and end the persisting questions about a lack of independence and politicization within the office.

The initial results over the past year suggest that Mr. Roth is restoring a culture of independence to the Office of Inspector General. For example, committee staff is aware of one incident where the Inspector General resisted an effort by a Department office to request that the OIG redact or classify the results of an audit of a cybersecurity program.[672] The Inspector General also made clear to all OIG employees that they should step forward to voice concerns about improper behavior, and blow the whistle to their supervisors or the Inspector General personally if need be.[673] On June 17th, Mr. Roth emailed all employees of DHS, encouraging them to take a "proactive role in improving DHS by reporting wrongdoing" and to "root out waste, fraud, and abuse," he further explained the whistleblower protections to safeguard employees from retribution.[674] The Inspector General has also sought the cooperation and assistance of

---

actively and openly sought the nomination to be the permanent IG and often spoke of his close relationship with her office and staff. The OIG allegedly reclassified a report on TSA Advanced Imaging Technology from TS to SCI in order to prevent access to the report. The former OIG also consulted with DHS General Counsel and not his own independent General Counsel, taking instructions about when to release an audit report.

[671] This issue is discussed in detail in the FCO subcommittee report. For example, under the former acting Inspector General, five OIG reports were withdrawn after it was found out that the former acting Inspector General's wife worked for the DHS Office of Program Accountability and Risk Management. These reports concerned contracts and acquisitions from Coast Guard, Federal Protective Services, and Customs and Border Protection. Despite the acting Inspector General recusing himself from his office's review process on these reports, they were never fully reinstated.

[672] An example of Mr. Roth's commitment to independence occurred when the Office of Inspector General was releasing its audit of the Department's Einstein E3A cybersecurity program. The audit identified problems within the program. The Committee staff learned that, immediately prior to the audit's release, the Department asked that sections of the report be redacted due to issues related to law enforcement sensitivities, which delayed the audits release, even though the National Protection Programs Directorate had already reviewed the audit and sent it back to the Inspector General without audit requests. Mr. Roth later told Committee staff in a briefing that the incident and the request was "bizarre" and subsequently released the audit with no redactions. Committee staff briefing with Inspector General John Roth, April 21, 2014.

[673] Email from John Roth, Inspector General, "Message from Inspector General," April 24, 2014. In part, the email addresses the FCO Subcommittee report that was released that day: "I appreciate those OIG employees who stepped forward to express their concerns to the Committee. Please be assured that you have a right to, and you should, bring improper behavior to the attention of someone who can do something about it. You can always speak to your supervisor, or if you are uncomfortable with that, bring it to our Ombudsperson, AIG Mike Beard, or if that doesn't work, to me personally."

[674] Email from John Roth, Inspector General, "Message from the Inspector General," June 17, 2014.

potential whistleblowers within the U.S. Secret Service as the OIG began its investigation of recently disclosed security breaches.[675]

Prior to Mr. Roth's arrival, the OIG made changes to its organizational structure to establish an Office of Integrity and Quality Oversight which is supposed to enhance the OIG's ability to execute functions such as receiving complaints and protecting whistleblowers. This division of the OIG has been enhanced under Mr. Roth's leadership by taking on the mission of conducting various oversight actions to ensure that other offices within the OIG remain independent.

Opportunities to Strengthen and Improve the Office of Inspector General

However, there are other areas where the Office of Inspector General could improve its management and operations to ensure its independence and improve its performance. For example, in September 2014, the Government Accountability Office presented an audit of the Office of Inspector General, identifying some problems and areas for improvement. GAO noted that the OIG's process for recording and referring complaints directly from DHS employees does not provide reasonable assurance that the whistleblowers' names and identifies would be protected from disclosure; for example, the online whistleblower hotline submission form required a submitter's name.[676] The OIG subsequently fixed this problem.

Questions also exist regarding whether the DHS Inspector General currently has the resources or practices in place to successfully investigate and mitigate the problem of corruption within the Department's workforce; including the problem of potentially widespread corruption within its workforce along the Southern border. For example, GAO found that the OIG had "not reached an agreement with the Federal Bureau of Investigation on coordinating and sharing border corruption information."[677] Such information sharing could assist both the OIG and FBI to improve their border corruption investigations. It is also not clear that the OIG's workforce is equipped to handle the number of corruption cases that have been open in the past, including in 2012 when the number of open corruption cases forced the Inspector General to transfer some

[675] Email from John Roth, Inspector General, "Message from Inspector General," October 8, 2014.
[676] Government Accountability Office, Inspectors General: DHS OIG's Structure, Policies and Procedures Are Consistent With Standards, but Areas for Improvements Exist, GAO-14-726, September 2014.
[677] Ibid.

cases back to components' offices of internal affairs.[678] More so than any other organization within the Department, reallocating additional resources to the Office of Inspector General could be the wisest investment that Congress and the Secretary could make.

One option that Congress could consider for strengthening the Office of Inspector General by making more resources available for its mission would be for Congress to pass legislation that would allow the Investigations Division to receive a percentage of assets forfeited as a result of their investigations.[679] There are currently three Offices of Inspectors General that have authority to participate in asset forfeiture, but the DHS OIG is not one.[680] The DHS OIG recovered approximately $25 million between October 1, 2013 and March 31, 2014.[681]

Another way to strengthen and improve the Inspector General's performance is to free the office of unnecessary congressional-mandates, which consume staff time and resources, and prevent the OIG from pursuing higher priority audits or investigations. Congress often includes in statutes directions for Offices of Inspectors General (OIG) to perform particular audits. The average OIG has approximately thirty percent of its workload mandated.[682] Inspector General Roth told Congress that the DHS-OIG faces a workload that is approximately 70 percent congressionally-mandated, more than double the typical amount.[683]

While congressionally mandated audits can be helpful, they also reduce the amount of time, money and resources that an office can spend conducting discretionary audits. According to the Inspector General, discretionary audits are the agency's "sweet spot of oversight" and provide the maximum impact.[684] Specifically, the DHS IG explained that discretionary audits provide greater deterrence, more flexibility, and the most value, because they allow the agency

---

[678] Ruben Gomez, "DHS IG partners with CBP, ICE to investigate workforce corruption," Federal News Radio, August 2, 2012.
[679] When the Federal Government uses asset forfeiture authority, it punishes and deters criminal activity by depriving criminals of property used or acquired through illegal activities. Certain law enforcement agencies participate in the Treasury Department's Treasury Forfeiture Fund or the Justice Department's Asset Forfeiture Fund. These agencies can use forfeited funds to pay expenses related to the investigation of illegal activities, such as contracting with forensic accountants who can reconstruct financial transactions and identify forfeitable assets in complex grant and procurement fraud cases.
[680] The Office of Inspectors General at USDA, DOD (DCIS) and Department of Transportation
[681] DHS OIG Semiannual Report to Congress, Department of Homeland Security, at: http://www.oig.dhs.gov/assets/SAR/OIG_SAR_Oct13_Mar14.pdf, accessed November 7, 2014, at p. 2.
[682] John Roth, Inspector General, Department of Homeland Security, statement made to Congressional staff, Department of Homeland Security, Office of the Inspector General Budget Briefing (March 11, 2014.)
[683] Department of Homeland Security, Office of the Inspector General, Budget Briefing Power Point, FY 2014 Projected to be Issued Reports By Origin, pg. 7 (March 11, 2014).
[684] Department of Homeland Security, Office of the Inspector General, Budget Briefing Power Point, Audits by Origin (March 11, 2014).

to identify opportunities for corrections *before* a crisis occurs.[685] In the 113th Congress, Senators Coburn and Carper sponsored legislation to eliminate some burdensome mandated requirements for the DHS OIG, which President Obama signed into law on December 18, 2014.[686] Despite the passage of this legislation, the DHS OIG will continue to face some unnecessary audits, since the Coburn-Carper bill was narrowed to ensure that the bill would pass by unanimous consent without any opposition from other committees that had jurisdiction over DHS.

Addressing Information Access Challenges

In August 2014, forty-seven Inspectors General signed a letter to congressional oversight leaders saying the Justice Department, the Peace Corps and the Chemical Safety Board had withheld information on the basis that it was privileged. The letter cited "potentially serious challenges to the authority of every Inspector General and our ability to conduct our work thoroughly, independently, and in a timely manner." The Inspector General Act of 1978 requires that inspectors general have "complete, unfiltered, and timely access to all information and materials … without unreasonable administrative burdens," according to the letter.[687] The officials said that watchdogs from other agencies have "faced similar obstacles to their work, whether on a claim that some other law or principle trumped the clear mandate of the IG Act or by the agency's imposition of unnecessarily burdensome administrative conditions on access."[688]

The Paperwork Reduction Act (PRA) also presents information acquisition challenges to the DHS OIG. The PRA was designed, among other things, to "ensure the greatest possible public benefit from and maximize the utility of information created, collected, maintained, used, shared and disseminated by or for the Federal Government" and to "improve the quality and use of Federal information to strengthen decision making, accountability, and openness in Government and society."[689] One example of how this affects the DHS OIG specifically is the current audit of FEMA's Staffing for Adequate Fire and Emergency Response (SAFER) grants to determine whether the grantees comply with grant requirements and guidance precluding

[685] Id.
[686] PL 113-284.
[687] Letter to House and Senate Oversight Chairs, August 5, 2014.
[688] Id.
[689] 44 U.S.C. § 3501

waste, fraud, and abuse of grant funds.[690] According to the PRA from which Offices of Inspectors General are not exempt, the survey for this audit must (1) seek public comment on proposed collections and (2) submit proposed collections for review and approval by the Office of Management and Budget (OMB).[691] It is possible this action could threaten the independence of the audit because OMB must approve the survey, or in other words, the audit's information collection tool. Additionally, the approval and public comment period will delay the work and affect the timeliness of the report. Congress should work to pass legislation that would exempt Offices of Inspectors General from the Paperwork Reduction Act, as such an exemption exists for the Government Accountability Office (GAO).

Improving DHS's Accountability to Implement OIG Recommendations

Questions also exist about how effective the OIG is in pushing the Department to address its recommendations. Currently, there are numerous recommendations and findings through OIG reports and audits that have not been addressed. As of July 2014,[692] there are 779 open recommendations, including one from 2002.[693] This shows that the Department is making progress implementing recommendations, since there were there were 1,239 open recommendations as of March 31, 2013. However, it is concerning that these recommendations remain open for such extended periods of time since the components generally concur with recommendations over ninety-five percent of the time.[694]

Transparency promotes accountability, and provides information for citizens about what their Government is doing. Information maintained by the Federal Government is a national asset. By making open recommendations available to the general public, this could force the Components to be more accountable to the public. Inspector General Roth has made strides to make the DHS's open recommendations more transparent by posting them on the

---

[690] Federal Register Notice, Agency Information Collection Activities: DHS OIG Audit of FEMA's Assistance to Firefighters Grant Program, DHS Form 530, DHS Form 531, DHS Form 532, October 2, 2014, https://www.federalregister.gov/articles/2014/10/02/2014-23513/agency-information-collection-activities-dhs-oig-audit-of-femas-assistance-to-firefighters-grant, accessed November 14, 2014.
[691] OMB Memorandum on Paperwork Reduction Act, April 7, 2010, http://www.whitehouse.gov/sites/default/files/omb/assets/inforeg/PRAPrimer_04072010.pdf, accessed November 7, 2014.
[692] According to the most recent available open recommendations report
[693] "DHS Open Recommendations" DHS Office of Inspector General, July 30, 2014; http://www.oig.dhs.gov/assets/Mgmt/2014/DHS_Open_Rec_Rep_073014.pdf, accessed October 2, 2014.
[694] Department of Homeland Security, Office of the Inspector General, Budget Briefing Power Point, FY 2014 Projected to be Issued Reports By Origin, p. 7.

DHS-OIG's website. However, the open recommendations report is not consistently updated on the IG's website. Between July 31, 2014 and December 15, 2014, the list was not updated, and therefore did not include over thirty-two issued reports with roughly 132 recommendations. The OIG's website design provides challenges to transparency as a whole as it is not user-friendly or search-friendly.

Opportunity to Reduce Duplication within the Department

The CIS Ombudsman office operates as an USCIS Inspector General for policy matters, while occasionally helping immigration applicants appeal to USCIS.[695] There is an obvious conflict for a government funded DHS entity representing alien petitioners. Additionally, USCIS frequently rejects and rarely implements the recommendations of the Ombudsman's office. The functions of the Ombudsman's office would be best served in the form of a grant to outside legal representation non-profit organizations or funding of outside entities to take on cases, essentially outsourcing the work.[696] The policy aspect of the office could be the work of the DHS OIG. While the CIS Ombudsman is a relatively small office, it could be consolidated into the work of the DHS Office of Inspector General.

Federal Law Enforcement Training Centers (FLETC)

The Federal Law Enforcement Training Centers (FLETC) were created in 1970 within the Department of the Treasury with a mission of creating standardized training for federal law enforcement officers and agents. In 2003, FLETC was transferred into the Department of Homeland Security. As FLETC Director Connie L. Patrick wrote in 2003, "the move reflected the centrality of the FLETC's mission in support [of the national strategy to guard against terrorism]."[697] That year, GAO reviewed FLETC programs, and identified capacity planning and

[695] CIS Ombudsman, Department of Homeland Security, at: http://www.dhs.gov/topic/cis-ombudsman, accessed December 31, 2014.
[696] USCIS Ombudsman Case Assistance, March 25, 2014, http://www.dhs.gov/case-assistance, accessed November 7, 2014.
[697] FLETC 2003 Annual Report, Department of Homeland Security, at: https://www.fletc.gov/sites/default/files/imported_files/reference/reports/annual-report/fy03-ann_ual-report.pdf, accessed December 30, 2014.

management oversight as key challenges for the component, and noted that DHS is planning to review FLETC training needs and capacities.[698]

The Department currently spends roughly $258 million annually[699] to operate FLETC, which operates four primary centers in Georgia, Maryland, New Mexico, and South Carolina, and also has presence at other law enforcement training programs in the United States and in foreign countries.[700] FLETC reports that it currently serves approximately 90 other federal agencies and its mission is "to train those who protect the homeland."[701] The Centers also train state, local, and tribal law enforcement officers.

Very little oversight work has been done to review the Federal Law Enforcement Training Centers and its programs. The DHS Inspector General has not conducted recent audits of its operational programs, and its most recent review of FLETC's financial management did not identify any significant problems.[702] Likewise, GAO has not conducted a complete audit of FLETC and its training programs and mission since its 2003 report.

Congress and the Department would benefit from additional oversight of the Centers to better understand their performance, and how the $258 million DHS spends on the program annually is improving the nation's ability to protect the homeland. Auditors should examine FLETC's programs, including those that are provided to state, local, and tribal partners, to determine their efficiency and effectiveness. The Congress and Department should also conduct a more thorough review of DHS's various assets devoted to training law enforcement officers and other DHS personnel to consider whether there are opportunities to achieve cost savings and efficiency by consolidating DHS's various training centers and programs. For example, several of DHS's other components operate their own training centers or academies outside of FLETC. In addition, Congress and the Department should evaluate other opportunities to create efficiencies between FLETC and other agencies' training missions, since approximately 90 other federal agencies use the Centers. For example, in September 2014, the Chairmen of the

---

[698] Government Accountability Office, "Federal Law Enforcement Training Center: Capacity Planning and Management Oversight Need Improvement," GAO-03-736, July 2003.
[699] Department of Homeland Security, Budget-in-Brief Fiscal Year 2015, p.143.
[700] "Locations," Federal Law Enforcement Training Centers, Department of Homeland Security, at: https://www.fletc.gov/locations, December 30, 2014, accessed December 30, 2014.
[701] "Our mission, vision and values," FLETC, Department of Homeland Security, at: https://www.fletc.gov/our-mission-vision-and-values, accessed December 30, 2014.
[702] DHS Office of Inspector General, Federal Law Enforcement Training Center[s'] Management Letter for FY2013 Financial Statements Audit, OIG-14-68, April 2014.

House Foreign Affairs Committee and the House Homeland Security Committees requested that the State Department halt plans to construct a new training center, and asked GAO to review the project plans to determine whether an expansion of FLETC would cost less while providing the services that the State Department needs.[703] DHS and FLETC reported that this strategy would save taxpayers $1 billion over ten years.[704]

[703] "Royce, McCaul, Duncan Request Review of State Department's plans to Construct New Security Training Center," House Foreign Affairs Committee, September 19, 2014.
[704] Ibid.

Part II: Recommendations

Based on his and others' oversight of the Department of Homeland Security over the past ten years, including the information presented in this report, Senator Tom Coburn offers the following recommendations for Congress and the Department of Homeland Security:

1. **Reforming DHS must begin by reforming Congress's approach to homeland security—including streamlining committee jurisdiction over DHS and putting aside parochial considerations when making policies for DHS.**

The biggest challenge facing the Department of Homeland Security is Congress itself. Congressional oversight of executive branch agencies is one of the essential features of our government, allowing the people, through their elected representatives, to hold agencies accountable for complying with and enforcing the law. Yet, when it comes to DHS, Congress's oversight of the Department is fractured, disorganized and, at times, contradictory.

Under the current jurisdictional rules, the Department of Homeland Security reports that it is accountable to responding to inquiries from more than 90 committees and subcommittees that have some jurisdiction to conduct oversight of DHS.[705] The Washington Post reported that the number of Committees that exercise some jurisdiction over DHS was "nearly three times the number that oversee the Department of Defense."[706] This means that hundreds of legislators across both bodies of Congress, including dozens of Committee chairs and ranking members, have the power to oversee, question, and set priorities for DHS.

This fractured jurisdiction creates challenges both for Congress and DHS. For example, authorization legislation is routine for government organizations, and is the mechanism by which Congress sets agency priorities and comprehensive policy direction. But jurisdictional

[705] This estimated has been attributed to the DHS Office of Legislative Affairs, and was cited by the Aspen Institute and Annenberg Public Policy Center of the University of Pennsylvania, in various publications since 2013. Committee staff sent an inquiry to CRS to clarify what was the most accurate estimate of number of committees and subcommittees that have jurisdiction over DHS. CRS reported that "there is no single accepted methodology for making an authoritative count, due in part to the flexibilities inherent in the rules and precedents of each chamber." Email from CRS to Committee Staff, December 17, 2014.

[706] Jerry Markon, "Department of Homeland Security has 120 reasons to want streamlined oversight," Washington Post, September 25, 2014.

overlap makes it almost impossible for Congress to enact a full legislative authorization of the Department, since it would require input or referral from dozens of committees and committee chairmen on both sides of the Capitol, and likely result in power shifting between the various committees involved. The result is that much of the policymaking for DHS is deferred to the Congressional appropriations committees, as well as the executive branch, to direct the Department's policies. For the Department, jurisdictional overlap results in its leadership being responsible for answering requests for information from and to testify before dozens of different committees.

Congress's dysfunctional approach to jurisdictional oversight has been a longstanding problem. In 2004, the 9/11 Commission warned that "so long as oversight is governed by current Congressional rules and resolutions, we believe that the American people will not get the security they want and need."[707] The findings of this report, including DHS's failure to achieve its mission, substantiate this decade-old warning.

Besides the significant problem of confused Congressional oversight of DHS, the nature of Congress and the interests that shape lawmakers' decisions creates a significant challenge to reform the DHS to allow it to focus on national priorities where it can yield the biggest improvement in national security. In an ideal world, every member of Congress would make every decision based on a single factor—what would be best for the nation? But we do not live in an ideal world, and the reality is that members of Congress often make decisions based on narrow or short-term factors, including what may benefit members' parochial interests.

As a result, DHS's programs are not always focused on addressing the most serious risks or yielding the greatest improvements in our nation's security. DHS's approach to providing preparedness grants and disaster relief—issues that are discussed previously in this report—are good examples of how politics shapes DHS's programs. For example, in 2004, then-DHS Secretary Tom Ridge admitted to Congress that political pressure to distribute funds affected the risk formula used for the Urban Areas Security Initiative program. When questioned about the risk formula and how grants were awarded, Ridge told Congress that he was looking for a formula that gets "218 votes in the House or 51 votes in the Senate, in order to get it done."[708]

---

[707] 9/11 Commission Report, p. 419.
[708] Secretary of Homeland Security Tom Ridge, Department of Homeland Security Oversight: Terrorism and Other Topics Federal, Hearing Transcript of Judiciary Committee, U.S. Senate, June 9, 2004.

Similarly, a majority of Senators voted down Senator Coburn's amendment in 2012, which would have required the Department of Homeland Security to update and replace its formula for deciding when the federal government should declare a disaster, which is biased towards less populated states like Oklahoma, and results in disasters often being declared after routine weather events. At least some of the Senators voting against reforming the disaster declaration process were likely interested in ensuring that funds continue to go to their state, rather than focusing relief on the biggest emergencies and natural disasters.

2. **Congress and the Department should refocus its programs and missions on national priorities and the Constitutional responsibilities of the federal government where the Department is the lead agency.**

Congress and DHS should review the evidence and the oversight work that has been done related to its current performance with respect to its five priority missions to reconsider, and refocus DHS's initiatives on national priorities and the federal government's responsibilities where DHS is the lead agency, consistent with the Constitution. Doing this will require recognition of what the Department is today, as well as what it is not, rather than allowing history and the momentum of the status quo to dictate DHS's future. For example, DHS has considered itself a counterterrorism agency since it was created; however, today it is clear, based on the oversight evidence reviewed in this report, that DHS's top mission is not preventing terrorist attacks. In fact, the Department appears to do little of this work, with other agencies taking lead responsibility for terrorism prevention. Moreover, too much of what the Department does is not focused on national priorities and clear responsibilities of the federal government, and these programs and activities should be ended. Regarding DHS's five priority missions, the following are recommendations for how DHS can refocus its programs on national priorities and federal responsibilities where the Departments in the lead agency:

- ***Reforming Counterterrorism and Protective Security.*** For its counterterrorism and protective security mission, the Department could yield the biggest value by focusing on areas where it is the lead agency or has unique assets and capabilities to support the national federal counterterrorism effort. These include: improving the Department's programs to secure the nation's borders, skies, and waterways, tracking and monitoring people entering

and exiting the country including to identify potential threats, and enforcing immigration law and improving the vetting of our immigration programs. DHS may also be uniquely positioned to provide value in domestic programs for countering violent extremism. Congress should also ensure that DHS effectively executes its protective security responsibilities for protecting national leaders and the federal government's assets.

- ***Securing and Managing Our Borders***: Border security is an area where DHS has the lead responsibility for the federal government, and this should be an area of reprioritization. A focus of DHS's border security initiatives should be to improve transparency about border security metrics to allow DHS, as well as state and local authorities, to swiftly work to close gaps in border security vulnerabilities, including by improving its use of existing resources. DHS should also be given authority to address the problem of potential corruption and weaknesses in its workforce. However, the surest way to improve the security of U.S. borders would be through a policy of deterrence—making clear to people seeking to trespass and enter our country illegally that the United States will enforce the rule of law and trespassers will be returned home.

- ***Enforcing and Administering Our Immigration Laws:*** Congress should reprioritize DHS's initiatives for enforcing and administering immigration laws, an area the Department has a lead federal responsibility. Congress should ensure that DHS meets its obligations for immigration administration and enforcement, including the swift and accurate processing of immigration benefits, thorough vetting of petitioners, and effective tracking of people entering and exiting the country, including monitoring and enforcing visa time limits. Moreover, DHS should be forced to meet its responsibility for upholding the rule of law, including removing illegal immigrants—particularly those that threaten public safety and domestic security. DHS's visa programs that have apparent criminal or national security vulnerabilities, including the Student Exchange and Visitor Program and EB-5 visa programs, should be reformed, suspended, or ended to mitigate potential vulnerabilities.

- ***Safeguarding and Securing Cyberspace:*** Congress should require DHS to focus on its basic responsibilities for securing its networks, practicing good cybersecurity, and assisting OMB

with its work to oversee federal civilian agencies' cybersecurity practices. DHS can provide value to the private sector, including owners and operators of critical infrastructure systems, by providing information about cybersecurity threats, and by facilitating the sharing of information between non-governmental entities. However, Congress should be cautious and realistic about what responsibilities DHS can and should provide for the private sector, given DHS's struggles with its own cybersecurity, and its work overseeing the private sector in other areas. Moving forward, Congress and the Department should reconsider DHS's strategy for cybersecurity—shifting from vulnerability mitigation, which is likely to prove ineffective in stopping the most serious threats, to supporting federal and private sector strategies for deterring adversaries.

- ***Strengthening National Preparedness and Resilience:*** Congress should refocus DHS's programs for disaster assistance and emergency management to restore an appropriate balance of responsibility between the federal government and states and localities. Specifically, Congress should reform FEMA's relief programs to reprioritize providing emergency assistance and relief when states and local communities have truly been overwhelmed and when American citizens' lives are at risk. Further, it should reform its flood insurance program to discourage, rather than encourage, people from building or rebuilding homes or properties where they are likely to be in harm's way. Moreover, Congress should end FEMA's wasteful and ineffective grant programs, which are not measurably reducing risk or improving domestic security, and instead have become yet another state and local subsidy program.

Reconsidering DHS's programs and refocusing on areas where DHS has a lead responsibility for a clear duty of the federal government also entails ending DHS's programs or initiatives that are unnecessary, ineffective, or duplicative of other federal, state, local or private sector initiatives.

3. **DHS's leaders responsible for executing its missions should be given the authority to manage and lead the Department, including strengthening DHS's culture, and be held responsible and accountable for its performance**

Since its creation, the Department of Homeland Security has struggled in the area of management, as well as directing and aligning the programs of it is many components, offices, and personnel. In 2003, GAO identified DHS management as a high-risk area due to the challenges of standing up and integrating the new department.[709] Ten years later, GAO reported that "while DHS has made important progress in implementing, transforming, strengthening and integrating its management functions," that DHS management "remains high risk because the department has significant work ahead," and that these challenges "hinder the Department's ability to meet its missions."[710] In November 2014, the DHS Inspector General reported that the Department continued to face major challenges in its management and performance, including operations integration, acquisitions management, and financial management.[711] The Inspector General warned that "Some of the most persistent challenges arise from the effort to combine and coordinate diverse legacy agencies into a single cohesive organization capable of fulfilling a broad, vital, and complex mission."[712]

One of the key areas where the Department and its leaders have struggled is in holding its employees accountable, a basic aspect of effective management. Oversight conducted by watchdogs, including the Inspector General and by Senator Coburn, identified multiple programs where there was significant waste, fraud, and abuse with little to no apparent accountability or consequences for DHS personnel responsible for managing those programs.

For example, the Inspector General issued a report in December 2013 which showed that DHS was not managing its Home-to-Work program, which provides one of the Department's approximately 56,000 vehicles to approximately 17,400 employees for use to drive from their

[709] Government Accountability Office, High Risk Series: An Update, GAO-13-283, February 2013.
[710] GAO stated, "DHS continues to face significant management challenges that hinder the department's ability to meet its missions," which resulted in significant performance problems and mission delays. Government Accountability Office, High Risk Series: An Update, GAO-13-283, February 2013
[711] The Inspector General reported that "the Department's major challenges were in the following areas: DHS operations integration, acquisitions management, financial management, IT management and privacy issues, transportation security, border security and immigration enforcement, grants management, employee accountability and integrity, infrastructure protection, cybersecurity, and insider threat." DHS Office of Inspector General, Major Management and Performance Challenges Facing the Department of Homeland Security, Department of Homeland Security, OIG-15-09, November 14, 2014.
[712] Ibid, p.1. The Inspector General reported that "the Department's major challenges were in the following areas: DHS operations integration, acquisitions management, financial management, IT management and privacy issues, transportation security, border security and immigration enforcement, grants management, employee accountability and integrity, infrastructure protection, cybersecurity, and insider threat." Ibid, p.1.

homes to their place of work.[713] In responses to questions asked by Senator Coburn, the Department provided additional information about the Home-to-Work program, which showed significant problems and that DHS headquarters did not have control over the program.[714] The Department acknowledged that its "lack of success in fully complying with [Home-to-Work] transportation requirements" was largely a result of the "complexity and inadequate direction of existing policy."[715] Although Secretary Johnson wisely issued a directive in August 2014 to curtail participation in the program, it is unclear whether managers within DHS that were responsible for the mismanagement of the Home-to-Work program were held accountable for the apparent waste, fraud, and abuse.

The Department's handling of its administratively uncontrollable overtime (AUO") pay program is another example of poor management and the absence of accountability. Courageous whistleblowers stepped forward, and reported to watchdogs that there was apparently widespread abuse of the Department's policy for providing overtime pay to some of its workers. The U.S. Office of Special Counsel (OSC) reported to Congress and the President the apparent problems with the program, including some employees regularly claiming two hours of improper AUO pay per day. "Such abuse of overtime pay is a violation of the public trust and a gross waste of scarce government funds," declared Carolyn Learner, the Office of Special Counsel.[716] In January 2014, Secretary Jeh Johnson wisely issued a memorandum suspending the use of AUO pay for many of the Department's employees, and initiated a Department-wide review of the program's management.[717] However, it is unclear where DHS personnel, including senior managers, were held accountable—including by termination of their jobs—for abusing and mismanaging this program, apparently for an extended period of time and at a significant cost to taxpayers.

The Department's continued struggles with management and leadership limits its ability to become a unified organization that is stronger and more effective because of the assets and capabilities of its many components and programs. The Department's headquarters consolidation project at the St. Elizabeths campus in the District of Columbia is emblematic of

[713] Office of Inspector General, "DHS Home-to-Work Transportation," Department of Homeland Security, OIG-14-21, December 2013.
[714] Letter from Acting Under Secretary for Management Chris Cummiskey to Senator Coburn, April 8, 2014.
[715] Ibid.
[716] Ms. Carolyn Lerner, U.S. Office of Special Counsel, Letter to the President of the United States, October 31, 2013.
[717] Josh Hicks, "Union opposes Homeland Security's overtime suspension," Washington Post, February 3, 2014.

these struggles. Announced in 2006, the headquarters' consolidation at the St. Elizabeths campus was planned to be complete by 2016, pending available funding from Congress. To date, more than $1.5 billion has been spent to complete 70 percent of the campus's infrastructure, and to build a new headquarters building for the Coast Guard, currently the sole occupant of the campus.[718] As of December 2014, it is not clear that DHS has a viable plan for the St. Elizabeths project, including a plan to yield cost savings by rendering many of DHS's leased properties unnecessary after consolidation. Particularly disconcerting is that, on its current path, DHS is unlikely to be able to consolidate its headquarters and component-level leadership on the campus, which would be the strongest argument for the project's completion. While DHS has faced funding constraints and Congress shoulders some responsibility, the ongoing St. Elizabeths project is symbolic of DHS's ongoing struggle to unify the Department, which remains incomplete.

In addition to improving management to strengthen the organization's efficiency and effectiveness, DHS's leadership also needs to improve the Department's culture, which has been a persistent challenge for the organization. Poor morale has been a problem for DHS throughout its history. DHS consistently has been identified as one of the worst places to work in the federal government. According to the Department's most recent survey, employee morale and satisfaction continued to decline in 2014.[719] Overall, only 41 percent of its employees were satisfied with DHS.[720] The survey data reveals some alarming findings, including that only 22 percent of DHS employees believe that "steps are taken to deal with a poor performer who cannot or will not improve."[721] On the positive side, the DHS employees' survey results show that the overwhelming majority of its employees believed in the agency's mission with more than 85 percent believing that the work they do is important.[722]

The vast gap between the percentage of employees at DHS who believe in the importance of their jobs versus the percentage who are satisfied with the Department overall

[718] Information provided from DHS to the Committee about the state of the St. Elizabeths project.
[719] Andi Medici, "DHS employee morale, satisfaction drops again in 2014," Federal Times, October 10, 2014, at: http://www.federaltimes.com/article/20141010/MGMT/310100013/DHS-employee-morale-satisfaction-drops-again-2014, accessed December 14, 2014.
[720] Department of Homeland Security, "2014 Federal Employee Viewpoint Survey Results," at: http://www.dhs.gov/sites/default/files/publications/2014_FEVS_Summary_Results_DHS.pdf , accessed December 14, 2014.
[721] Ibid.
[722] Ibid.

suggests that there is an opportunity to change the organization's culture. However, doing so will require leadership. In his first year, Secretary Jeh Johnson has demonstrated that he recognizes that leadership, management, and Department-wide coordination and accountability are areas that must be addressed. His "Unity of Effort" initiative is well-intended, and an important step toward requiring DHS's headquarters leaders to hold its components and employees accountable. However, this area will likely remain a challenge for Secretary Johnson and his team, and Congress should consider ways to strengthen DHS leadership's ability to manage its components, hold its components and employees accountable, and fundamentally change the Department's culture.

4. DHS's must focus on respecting American citizens' constitutional rights and focusing on the proper role of the federal government to restore and earn their trust. This is an area where vigorous and sustained oversight by Congress and other watchdogs is essential.

DHS and its component agencies are empowered to intrude on Americans' notions of privacy and freedom to an extent shared by very few other federal agencies. Put another way, law-abiding Americans are required to submit to a level of intimacy with the Department, on an everyday basis, that is unlike their relationship with most other federal agencies. Many of the Department's programs require engaging with the American public, and other U.S. persons, in a manner that may affect their privacy and lives, from screening and patting us down at the airport to conducting domestic intelligence and law enforcement operations; to screening Internet traffic to federal agencies' networks.

Over the past decade, there have been many questions about whether DHS was sufficiently respecting American citizens' constitutional rights and privacy. For example, Americans have questioned the appropriateness of the screening procedures that have been implemented to mitigate the recognized threat of terrorist attacks against commercial aviation, including TSA pat-downs and past deployment of screening technologies that produce revealing images of passengers.[723] There have also been many questions about whether DHS's domestic

[723] Many questions were asked about the efficacy, privacy, and safety of the backscatter x-ray scanners. For example, in January 2012, a bipartisan group of Senators from the Senate Homeland Security and Governmental Affairs Committee introduced legislation requiring an independent study of the machines and warning sides to be added at airports. "Senator Collins, Akaka, Levin, Coburn, Scott Brown Introduce Bill to Require Study, Warning

intelligence programs, including whether the government was spying and collecting information on its citizens, including information about activities that are protected under the First Amendment of the U.S. Constitution.[724] There are also open questions about DHS's law enforcement programs and whether DHS's officers have used force excessively[725] or in a manner beyond the proper role of a federal law enforcement agency.[726] Other questions exist about whether DHS's grant programs contribute to excessive or improper use of force by state and local law enforcement authorities.[727] There have also been questions about whether DHS is adequately safeguarding sensitive and personal information that it maintains to protect Americans' privacy.[728]

Addressing these concerns will require sustained focus and attention by the Department, Congress, and others who must hold it accountable. For its part, the Department must ensure that proper policies and procedures are in place to ensure that all programs are operating in a manner that respects Americans' constitutional rights. This includes requiring adequate training for personnel to ensure that they are complying with policies regarding civil rights and

---

of Health Effects of Some Airport Scanners," Senate Homeland Security and Governmental Affairs Committee, January 31, 2012. TSA's other screening procedures, including pat downs, have been the focus of media attention over the past decade.

[724] Oversight work done by Senator Coburn, for example, has identified areas where DHS was not ensuring that all programs are operating in a manner that ensures that all Americans' constitutional rights were protected. For example, the bipartisan PSI investigation of DHS's support for the state and local fusion center program found that DHS and its intelligence officers faced challenges ensuring that its intelligence products were not reporting information related to protected activities under the First Amendment of the Constitution. Permanent Subcommittee on Investigations, "Federal Support for and Involvement in State and Local Fusion Centers: Majority and Minority Staff Report," October 3, 2012.

[725] CBP's use of force policies have been the focus of questions, due in part to the number of people killed by DHS officers in the line of duty. In 2014, the American Civil Liberties Union filed a lawsuit to seek CBP's internal review of use of force incidents. See: Bob Ortega, "ACLU sues to get report critical of CBP's use of force," Arizona Republic, May 23, 2014. On March 7, 2014, the Department announced and released a new Use-of-Force policy guidelines for DHS, CBP, and ICE. See: DHS Press Office, "DHS, CBP, ICE Release Use-of-Force Policies," March 7, 2014.

[726] Senator Tom Coburn has sent multiple inquiries to ICE raising questions about investigative operations and whether Homeland Security Investigations are appropriate for the federal government's authorities, including the October incident in Kansas City, where HSI agents raided a women's clothing store discussed earlier in this report

[727] For example, the Senate Homeland Security and Governmental Affairs Committee examined the issue of whether DHS's grant programs were contributing to the problem of increasing militarization of state and local law enforcement. "Oversight of Federal Programs for Equipping State and Local Law Enforcement," Senate Homeland Security and Governmental Affairs Committee hearing, September 9, 2014. Senator Coburn also presented evidence showing that states and localities were using funds provided by DHS's grant programs to acquire equipment, including armored vehicles and long range acoustic devices that may contribute police militarization and excessive force. See: Senator Tom Coburn, Safety at Any Price: Assessing the Impact of Homeland Security Spending in U.S. Cities, December 2012.

[728] For example, the DHS Inspector General identified "IT Management and Privacy Issues" as one of its major management and performance challenges. See: Office of Inspector General, "Major Management and Performance Challenges Facing the Department of Homeland Security," Department of Homeland Security, OIG-15-09, November 14, 2014.

civil liberties. Moreover, the Department should review its law enforcement and investigative programs to ensure that current policies and procedures are consistent with the Constitution, and do not contribute to abuses of authority that may threaten the American people's rights. For example, Congress and DHS should reform the allowable uses of its grant programs, including the equipment that it allows its grant recipients to purchase using federal funds through the preparedness grant programs (if the grants are continued) to ensure that federal funds do not contribute to excessive use of force by state and local law enforcement authorities.[729]

One way that the Department can earn the American people's trust is by improving transparency about its programs and operations. This can be done by being a more transparent partner with Congress—providing information in response to Congressional inquiries in a thorough and timely manner—to allow Congress to ask questions and verify that DHS's programs are not trespassing on Constitutional rights or privacy. DHS could also implement policies and procedures to create transparency and accountability for its employees involved in law enforcement and security operations. For example, DHS officers involved with law enforcement operations, such as Border Patrol, ICE, CBP and others, could be required to use body cameras to demonstrate that employees are operating in a manner consistent with Departmental policy.

Vigorous and sustained independent oversight of the Department's activities is also critical. Congress and other watchdogs, such as the Inspector General, must do their part to continue to hold the Department accountable for adhering to the Constitution and not threatening to trespass on the American people's rights. Where concerns over the Department's activities may be misplaced, rigorous oversight is also a helpful way to alleviate these concerns by presenting facts to the American public. For example, some members of the American public have had questions about DHS's acquisitions of ammunition over the past few years. Senator Coburn and other watchdogs conducted oversight to determine whether DHS's level of ammunition acquisitions was appropriate, presenting evidence of their findings to the American people. For example, Senator Coburn published on his website the information that DHS provided about its ammunitions purchases in response to a November 13, 2012 letter, after many

[729] Senator Coburn introduced legislation (S. 2904, the Stop Militarizing Law Enforcement Act) in the 113th Congress. It includes legislative changes to reform DHS's grant programs.

constituents contacted his office with questions.[730] A GAO audit released in January 2014 found that DHS's ammunition purchases had actually declined since 2009.[731] GAO also found that DHS's purchases were comparable with those of the Department of Justice and were being managed effectively.[732]

[730] "Dr. Coburn Releases Correspondence with DHS Regarding Ammunition Purchases," The Office of Senator Tom Coburn, July 18, 2013.
[731] Government Accountability Office, "Department of Homeland Security: Ammunition Purchases Have Declined Since 2009," GAO-14-119, January 2014, at: http://www.gao.gov/assets/670/660143.pdf. (Accessed December 14, 2014.)
[732] Government Accountability Office, "Department of Homeland Security: Ammunition Purchases Have Declined Since 2009," GAO-14-119, January 2014, at: http://www.gao.gov/assets/670/660143.pdf. (Accessed December 14, 2014.)

Conclusion

The nation continues to face a fiscal crisis. The national debt exceeds $18 trillion. On the current course, the federal government's debt will continue to grow as the federal government continues to borrow and spend more than it collects in taxes and revenues and as more of the nation's long-term obligations and promises come due. The basic choice facing Congress and our leaders is whether we will dramatically increase the tax burden on current and future generations, inflate or devalue our currency and the American public's savings to minimize our debts, or sensibly reform the federal government's programs.

When it comes to reforming the government's programs, the Department of Homeland Security should be at the top of Congress's "to do" list. DHS is responsible for some of the federal government's most important responsibilities, including preventing terrorist attacks, securing our borders, skies, waterways, and transportation systems, protecting national leaders and assets, administering and enforcing our immigration laws, and responding to national emergencies. Yet the evidence available from ten years of oversight presented in this report shows that DHS is not successfully executing its key missions.

Reconsidering and reforming the Department of Homeland Security and its programs is a historic opportunity for Congress, the executive branch, and the American public. Refocusing DHS on the national priorities and federal responsibilities where the Department is the lead agency and empowering DHS's leadership to execute its missions effectively and in a manner consistent with the Constitution will strengthen our nation's security, improve our stewardship of resources, and demonstrate that our nation is committed to meeting its challenges.