Congressional Research Service
Informing the legislative debate since 1914

Selected Homeland Security Issues in the 116th Congress

Updated August 14, 2019

Congressional Research Service
https://crsreports.congress.gov
R45701

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

SUMMARY

R45701

August 14, 2019

William L. Painter, Coordinator
Specialist in Homeland Security and Appropriations

Selected Homeland Security Issues in the 116th Congress

In 2001, in the wake of the terrorist attacks of September 11, "homeland security" went from being a concept discussed among a relatively small cadre of policymakers and strategic thinkers to one broadly discussed among policymakers, including a broad swath of those in Congress. Debates over how to implement coordinated homeland security policy led to the passage of the Homeland Security Act of 2002 (P.L. 107-296), the establishment of the Department of Homeland Security (DHS), and extensive legislative activity in the ensuing years.

Initially, homeland security was largely seen as counterterrorism activities. Today, homeland security is a broad and complex network of interrelated issues, in policymaking terms. For example, in its executive summary, the Quadrennial Homeland Security Review issued in 2014 delineated the missions of the homeland security enterprise as follows: prevent terrorism and enhance security; secure and manage the borders; enforce and administer immigration laws; safeguard and secure cyberspace; and strengthen national preparedness and resilience.

This report compiles a series of Insights by CRS experts across an array of homeland security issues that may come before the 116th Congress. Several homeland security topics are also covered in CRS Report R45500, *Transportation Security: Issues for the 116th Congress*.

The information contained in the Insights only scratches the surface of these selected issues. Congressional clients may obtain more detailed information on these topic and others by contacting the relevant CRS expert listed in CRS Report R45684, *Selected Homeland Security Issues in the 116th Congress: CRS Experts*.

Contents

The Budget and Homeland Security 1
The U.S. Intelligence Community 2
Homeland Security Research and Development 4
National Strategy for Counterterrorism 6
Energy Infrastructure Security 7
U.S. Secret Service Protection of Persons and Facilities 9
Protection of Executive Branch Officials 11
Drug Trafficking at the Southwest Border 12
Border Security Between Ports of Entry 14
National Preparedness Policy 16
Disaster Housing Assistance 17
The Disaster Recovery Reform Act 19
The National Flood Insurance Program (NFIP) 21
National Flood Insurance Program (NFIP) Reauthorization and Reform 23
Community Disaster Loans 25
Firefighter Assistance Grants 27
Emergency Communications 28
U.S. National Health Security 30
Cybersecurity 32
Department of Homeland Security Human Resources Management 34
DHS Unity of Effort 36

Figures

Figure 1. HHS Secretary's Operations Center (SOC), Activated for the Wannacry Ransomware Attack, May 2017 31

Tables

Table 1. Comparison of Trump and Obama Counterterrorism Strategies 7

Contacts

Author Information 39

The Budget and Homeland Security

(William L. Painter; February 28, 2019)

Congress at times has sought to ascertain how much the government spends on securing the homeland, either in current terms or historically. Several factors compromise the authoritativeness of any answer to this question. One such complication is the lack of a consensus definition of what constitutes homeland security, and another is that homeland security activities are carried out across the federal government, in partnership with other public and private sector entities. This insight examines those two complicating factors, and presents what information is available on historical homeland security budget authority and current DHS appropriations.

Defining Homeland Security

No statutory definition of homeland security reflects the breadth of the current enterprise. The Department of Homeland Security is not solely dedicated to homeland security missions, nor is it the only part of the federal government with homeland security responsibilities.

The concept of homeland security in U.S. policy evolved over the last two decades. Homeland security as a policy concept was discussed before the terrorist attacks of September 11, 2001. Entities like the Gilmore Commission and the Hart-Rudman Commission discussed the need to evolve national security thinking in response to the increasing relative risks posed by nonstate actors, including terrorist groups. After 9/11, policymakers concluded that a new approach was needed to address these risks. A presidential council and department were established, and a series of presidential directives were issued in the name of "homeland security." These efforts defined homeland security as a response to terrorism. Later, multilevel government responses to disasters such as Hurricane Katrina expanded the concept of homeland security to include disasters, public health emergencies, and other events that threaten the United States, its economy, the rule of law, and government operations. Some criminal justice elements could arguably be included in a broad definition of homeland security. This evolution of the concept of homeland security made it distinct from other federal government security operations such as homeland defense.

Homeland defense is primarily a Department of Defense (DOD) activity and is defined by DOD as "... the protection of U.S. sovereignty, territory, domestic population, and critical defense infrastructure against external threats and aggression, or other threats as directed by the President." Homeland security, on the other hand, is a more broadly coordinated effort, involving not only military activities, but the operations of civilian agencies at all levels of government.

The Federal Homeland Security Enterprise

The Homeland Security Act of 2002 established the Department of Homeland Security (DHS). The department was assembled from components pulled from 22 different government agencies and began official operations on March 1, 2003. Since then, DHS has undergone a series of restructurings and reorganizations to improve its effectiveness.

Although DHS does include many of the homeland security functions of the federal government, several of these functions or parts of these functions remain at their original executive branch agencies and departments, including the Departments of Justice, State, Defense, and Transportation. Not all of the missions of DHS are officially "homeland security" missions. Some DHS components have legacy missions that do not directly relate to conventional homeland security definitions, such as the Coast Guard, and Congress has in the past debated whether FEMA and its disaster relief and recovery missions belong in the department.

Analyzing Costs Across Government

Section 889 of the Homeland Security Act of 2002 required the President's annual budget request to include an analysis of homeland security funding across the federal government—not just DHS. This requirement remained in effect through the FY2017 funding cycle. The resulting data series, which included agency-reported data on spending in three categories—preventing and disrupting terrorist attacks; protecting the American people, critical infrastructure, and key resources; and responding to and recovering from incidents—provides a limited snapshot of the scope of the federal government's investment in homeland security.

According to these data, from FY2003 through FY2017, the entire U.S. government directed roughly $878 billion (in nominal dollars of budget authority) to those three mission sets. Annual budget authority rose from roughly $41 billion in FY2003 to a peak in FY2009 of almost $74 billion. After that peak, reported annual homeland security budget authority hovered between $66 billion and $73 billion. Thirty different agencies reported having some amount of homeland security budget authority.

One can compare this growth in homeland security budget authority to the budget authority provided to DHS. The enacted budget for DHS rose from an Administration-projected $31.2 billion in FY2003, to almost $68.4 billion in FY2017.

FY2019 DHS Appropriations

For FY2019, the Trump Administration initially requested almost $75 billion in budget authority for DHS, including over $47 billion in adjusted net discretionary budget authority through the appropriations process. This included almost $7 billion to pay for the costs of major disasters under the Stafford Act. The Administration requested additional Overseas Contingency Operations (OCO) funding for the Coast Guard as a transfer from the U.S. Navy. Neither the Senate nor the House bill reported out of their respective appropriations committees in response to that request received floor consideration.

Continuing appropriations expired on December 21, 2018, leading to a 35-day partial shutdown of federal government components without enacted annual appropriations—including DHS. This was the longest such shutdown in the history of the U.S. government. On February 15, the President signed into law P.L. 116-5, which included the FY2019 DHS annual appropriations act. The act included almost $56 billion in adjusted net discretionary budget authority, including $12 billion for the costs of major disasters, and $165 million for Coast Guard OCO funding.

The current budget environment may present challenges to homeland security programs and DHS going forward. The funding demands of ongoing capital investment efforts, such as the proposed border wall and ongoing recapitalization efforts, and staffing needs for cybersecurity, border security, and immigration enforcement, may compete with one another for limited funding across the government and within DHS.

The U.S. Intelligence Community

(Michael E. DeVine; February 1, 2019)

Intelligence support of homeland security is a primary mission of the entire Intelligence Community (IC). In fulfilling this mission, changes to IC organization and process, since 9/11, have enabled more integrated and effective support than witnessed or envisioned since its inception. The terrorist attacks of 9/11 revealed how barriers between intelligence and law

enforcement, which originally had been created to protect civil liberties, had become too rigid, thus preventing efficient, effective coordination against threats. In its final report, the Commission on Terrorist Attacks upon the United States (the *9/11 Commission*) identified how these barriers contributed to degrading U.S. national security. The findings resulted in Congress and the executive branch enacting legislation and providing policies and regulations designed to enhance information sharing across the U.S. government.

The Homeland Security Act of 2002 (P.L. 107-296) gave the Department of Homeland Security (DHS) responsibility for integrating law enforcement and intelligence information relating to terrorist threats to the homeland. Provisions in the Intelligence Reform and Terrorist Prevention Act (IRTPA) of 2004 (P.L. 108-458) established the National Counterterrorism Center (NCTC) as the coordinator at the federal level for terrorism information and assessment and created the position of Director of National Intelligence (DNI) to provide strategic management across the 17 organizational elements of the IC. New legal authorities accompanied these organizational changes. At the federal, state, and local levels, initiatives to improve collaboration across the federal government include the FBI-led Joint Terrorism Task Forces (JTTFs) and, more recently, the DHS National Network of Fusion Centers (NNFC).

Within the IC, the FBI Intelligence Branch (FBI/IB), and DHS's Office of Intelligence and Analysis (OIA), and the Coast Guard Intelligence (CG-2) enterprise, are most closely associated with homeland security. OIA combines information collected by DHS components as part of their operational activities (i.e., those conducted at airports, seaports, and the border) with foreign intelligence from the IC; law enforcement information from federal, state, local, territorial and tribal sources; and private sector data about critical infrastructure and strategic resources. OIA analytical products focus on a wide range of threats to the homeland to include foreign and domestic terrorism, border security, human trafficking, and public health. OIA's customers range from the U.S. President to border patrol agents, Coast Guard personnel, airport screeners, and local first responders. Much of the information sharing is done through the NNFC—with OIA providing personnel, systems, and training.

The Coast Guard Intelligence (CG-2) enterprise is the intelligence component of the United States Coast Guard (USCG). It serves as the primary USCG interface with the IC on intelligence policy, planning, budgeting and oversight matters related to maritime security and border protection. CG-2 has a component Counterintelligence Service, a Cryptologic Group, and an Intelligence Coordination Center to provide analysis and supporting products on maritime border security. CG-2 also receives support from field operational intelligence components including the Atlantic and Pacific Area Intelligence Divisions, Maritime Intelligence Fusion Centers for the Atlantic and Pacific, and intelligence staffs supporting Coast Guard districts and sectors.

FBI/IB includes four component organizations:

- The Directorate of Intelligence has responsibility for all FBI intelligence functions, and includes intelligence elements and personnel at FBI Headquarters in field divisions.
- The Office of Partner Engagement develops and maintains intelligence sharing relationships across the IC, and with state, local, tribal, territorial, and international partners.
- The Office of Private Sector conducts outreach to businesses impacted by threats to vulnerable sectors of the economy such as critical infrastructure, the supply chain, and financial institutions.
- Finally, the Bureau Intelligence Council provides internal to the FBI a forum for senior-level dialogue on integrated assessments of domestic threats.

While the intelligence organizations of FBI and DHS are the only IC elements solely dedicated to intelligence support of homeland security, all IC elements, to varying degrees, have some level of responsibility for the overarching mission of homeland security. For example, in addition to NCTC, the Office of the DNI (ODNI) includes the Cyber Threat Intelligence Integration Center (CTIIC). It was established in 2015 and is responsible at the federal level for providing *all-source analysis* of intelligence relating to cyber threats to the United States. Much like NCTC for terrorism, CTIIC provides outreach to other intelligence organizations across the federal government and at the state, and local levels to facilitate intelligence sharing and provide an integrated effort for assessing and providing warning of cyber threats to the homeland.

IC organizational developments since 9/11 underscore the importance of adhering to privacy and civil liberties protections that many feared might be compromised by the more integrated approach to intelligence and law enforcement. This is particularly true considering the changing nature of the threat: The focus of intelligence support of homeland security has evolved from state-centric to increasingly focusing on nonstate actors, often individuals acting alone or as part of a group not associated with any state. Collecting against these threats, therefore, requires strict adherence to intelligence oversight rules and regulations, and annual training by the IC workforce for the protection of privacy and civil liberties.

Homeland Security Research and Development

(Daniel Morgan; June 21, 2019)

Overview

In the Department of Homeland Security (DHS), the Directorate of Science and Technology (S&T) has primary responsibility for establishing, administering, and coordinating research and development (R&D) activities. The Domestic Nuclear Detection Office (DNDO) is responsible for R&D relating to nuclear and radiological threats. Several other DHS components, such as the Coast Guard, also fund R&D and R&D-related activities associated with their missions. The Common Appropriations Structure that DHS introduced in its FY2017 budget includes an account titled Research and Development in seven different DHS components. Issues for DHS R&D in the 116th Congress may include coordination, organization, and impact.

Coordination of R&D

The Under Secretary for S&T, who leads the S&T Directorate, has statutory responsibility for coordinating homeland security R&D both within DHS and across the federal government (6 U.S.C. §182). The Director of DNDO also has an interagency coordination role with respect to nuclear detection R&D (6 U.S.C. §592). Both internal and external coordination are long-standing congressional interests.

Regarding internal coordination, the Government Accountability Office (GAO) concluded in a 2012 report that because so many components of the department are involved, it is difficult for DHS to oversee R&D department-wide. In January 2014, the joint explanatory statement for the Consolidated Appropriations Act, 2014 (P.L. 113-76) directed DHS to implement and report on new policies for R&D prioritization. It also directed DHS to review and implement policies and guidance for defining and overseeing R&D department-wide. In July 2014, GAO reported that DHS had updated its guidance to include a definition of R&D and was conducting R&D portfolio reviews across the department, but that it had not yet developed policy guidance for DHS-wide R&D oversight, coordination, and tracking. In December 2015, the joint explanatory statement

for the Consolidated Appropriations Act, 2016 (P.L. 114-113) stated that DHS "lacks a mechanism for capturing and understanding research and development (R&D) activities conducted across DHS, as well as coordinating R&D to reflect departmental priorities." In March 2019, GAO reported that the S&T Directorate had "strengthened its R&D coordination efforts across DHS, but some challenges remain," including that not all DHS components participate fully in the coordination mechanism that S&T has established.

A challenge for external coordination is that the majority of homeland security-related R&D is conducted by other agencies, most notably the Department of Defense and the Department of Health and Human Services. The Homeland Security Act of 2002 directs the Under Secretary for S&T, "in consultation with other appropriate executive agencies," to develop a government-wide national policy and strategic plan for homeland security R&D (6 U.S.C. §182), but no such plan has ever been issued. Instead, the S&T Directorate has developed R&D plans with selected individual agencies, and the National Science and Technology Council (a coordinating entity in the Executive Office of the President) has issued government-wide R&D strategies in selected topical areas, such as biosurveillance.

Organization for R&D

DHS has reorganized its R&D-related activities several times. In December 2017, it established a new Countering Weapons of Mass Destruction Office (CWMDO), consolidating DNDO, most functions of the Office of Health Affairs (OHA), and some other elements. DNDO and OHA were themselves both created, more than a decade ago, largely by reorganizing elements of the S&T Directorate. The Countering Weapons of Mass Destruction Act of 2018 (P.L. 115-387) expressly authorized the establishment and activities of CWMDO. The 116th Congress may examine the implementation of that act.

The organization of DHS laboratory facilities may also be a focus of attention in the 116th Congress. At its establishment, the S&T Directorate acquired laboratories from other departments, including the Plum Island Animal Disease Center (from the Department of Agriculture, USDA) and the National Urban Security Technology Laboratory, then known as the Environmental Measurements Laboratory (from the Department of Energy). It subsequently absorbed some laboratory facilities from other DHS components (such as the Transportation Security Laboratory from the Transportation Security Administration), but other DHS components retained their own laboratories (such as the U.S. Coast Guard Research and Development Center). During the 115th Congress, the Federal Bureau of Investigation agreed to assume some of the operational costs of the S&T Directorate's National Biodefense Analysis and Countermeasures Center, and DHS proposed to transfer operational responsibility for the National Bio and Agro-Defense Facility (NBAF)—a biocontainment laboratory currently being built by the S&T Directorate in Manhattan, Kansas—to USDA. In June 2019, DHS and USDA signed a memorandum of agreement outlining their plans for the NBAF transfer, and USDA released a strategic vision for the future of the facility.

Impact of R&D Results

In testimony at a Senate hearing in 2018, the Administration's nominee to be Under Secretary for S&T described the S&T Directorate's mission as "to deliver results" and referred to "timely delivery and solid return on investment." Members of Congress and other stakeholders have sometimes questioned the impact of DHS R&D programs and whether enough of their results are ultimately implemented in products actually used in the U.S. homeland security enterprise. Part of the debate has been about finding the right balance between near-term and long-term goals. In

testimony at House hearing in 2017, a former Under Secretary for S&T stated that the directorate "has worked hard to focus on being highly relevant—shifting from the past focus on long-term basic research to near-term operational impact." Yet testimony from an industry witness at the same House hearing stated that "there is a perception among some in the industry that S&T programs only infrequently significantly impact the operational or procurement activities of the DHS components." The 116th Congress may continue to examine the effectiveness and impact of DHS R&D.

National Strategy for Counterterrorism

(John W. Rollins, January 29, 2019)

On October 4, 2018, President Trump released his Administration's first National Strategy for Counterterrorism. The overarching goal of the strategy is to "defeat the terrorists who threaten America's safety, prevent future attacks, and protect our national interests." In describing the need for this strategy, National Security Advisor John Bolton stated that the terrorist "landscape is more fluid and complex than ever" and that the strategy will not "focus on a single organization but will counter all terrorists with the ability and intent to harm the United States, its citizens and our interests." The strategy states that a "*new approach"* will be implemented containing six primary thematic areas of focus: (1) pursuing terrorists to their source; (2) isolating terrorists from their sources of support; (3) modernizing and integrating the United States' counterterrorism authorities and tools; (4) protecting American infrastructure and enhancing resilience; (5) countering terrorist radicalization and recruitment; and (6) strengthening the counterterrorism abilities of U.S. international partners. In announcing the strategy, President Trump stated, "When it comes to terrorism, we will do whatever is necessary to protect our Nation."

In contrast, former President Obama's final National Strategy for Counterterrorism, published on June 28, 2011, primarily focused on global terrorist threats emanating from Al Qaeda and associated entities. The overarching goal of this strategy was to "disrupt, dismantle, and eventually defeat Al Qaeda and its affiliates and adherents to ensure the security of our citizens and interests." This strategy stated that the "preeminent security threat to the United States continues to be from Al Qaeda and its affiliates and adherents." The strategy focused on the threats posed by geographic dispersal of Al Qaeda, its affiliates, and adherents, and identified principles that would guide United States counterterrorism efforts: Adhering to Core Values, Building Security Partnerships, Applying Tools and Capabilities Appropriately, and Building a Culture of Resilience. In announcing the release of this strategy, President Obama included a quote from the speech he gave announcing the killing of Osama Bin Laden, "As a country, we will never tolerate our security being threatened, nor stand idly by when our people have been killed. We will be relentless in defense of our citizens and our friends and allies. We will be true to the values that make us who we are. And on nights like this one, we can say to those families who have lost loved ones to Al Qaeda's terror: Justice has been done."

Since President Trump's Counterterrorism Strategy was published, many security observers have pointed to the similarities and differences between the two Administration's approaches to counterterrorism. **Table 1**, below, presents the language contained in each strategy identifying major thematic aspects of the two counterterrorism strategies.

Table 1. Comparison of Trump and Obama Counterterrorism Strategies

Focus Area	Trump 2018 Strategy	Obama 2011 Strategy
Threat Actors	Numerous radical Islamists, revolutionaries, nationalists, separatists, and domestic groups.	Al Qaeda and its affiliates and adherents.
Geographic Focus	Global (including the United States)	Global (including the United States)
Primary Entities Responsible for Addressing the Threat	U.S. military, law enforcement, intelligence community, civilian government institutions, private sector, civil society, and international partners, and the American people.	U.S. Intelligence Community, military, law enforcement, allies, partners, and multilateral institutions.
Core Principles Pursued to Counter the Threat	Pursue terrorists at their source; isolate terrorists from financial, material, and logistical support; modernize and integrate counterterrorism tools and authorities; protect U.S. infrastructure and enhance preparedness; counter radicalization and recruitment; and strengthen the abilities of international partners.	Adhering to U.S. values, building security partnerships, applying counterterrorism tools and capabilities appropriately, and building a culture of resilience.
Balancing Terrorism-Related Activities and Safeguarding Rights	By sharing identity information and exploiting publicly available information, such as social media, the United States will identify these terrorists and enable law enforcement action against them in their home countries. In these efforts, the United States will take appropriate steps to protect privacy, civil rights, and civil liberties.	By ensuring that counterterrorism policies and tools are narrowly tailored and applied to achieve specific, concrete security gains, the United States will optimize its security and protect the liberties of its citizens.
Desired End State	The terrorist threat to the United States is eliminated, borders and all ports of entry into the United States are secure against terrorist threat, terrorism, radical Islamic ideologies, and other violent extremist ideologies do not undermine the American way of life, and foreign partners address terrorist threat so that these threats do not jeopardize the collective interests of the United States and our partners.	To defeat Al Qaeda, we must define with precision and clarity who we are fighting, setting concrete and realistic goals tailored to the specific challenges we face in different regions of the world. As we apply every element of American power against Al Qaeda, success requires a strategy that is consistent with U.S. core values as a nation and as a people.

Source: Comparison offered by CRS.

Energy Infrastructure Security

(Paul Parfomak; March 1, 2019)

Ongoing threats against the nation's natural gas, oil, and refined product pipelines have heightened concerns about the security risks to these pipelines, their linkage to the electric power

sector, and federal programs to protect them. In a December 2018 study, the Government Accountability Office (GAO) stated that, since the terrorist attacks of September 11, 2001, "new threats to the nation's pipeline systems have evolved to include sabotage by environmental activists and cyber attack or intrusion by nations." In a 2018 *Federal Register* notice, the Transportation Security Administration stated that it expects pipeline companies will report approximately 32 "security incidents" annually—both physical and cyber. The Pipeline and LNG Facility Cybersecurity Preparedness Act (H.R. 370, S. 300) would require the Secretary of Energy to enhance coordination among government agencies and the energy sector in pipeline security; coordinate incident response and recovery; support the development of pipeline cybersecurity applications, technologies, demonstration projects, and training curricula; and provide technical tools for pipeline security.

Pipeline Physical Security

Congress and federal agencies have raised concerns since at least 2010 about the physical security of energy pipelines, especially cross-border oil pipelines. These security concerns were heightened in 2016 after environmentalists in the United States disrupted five pipelines transporting oil from Canada. In 2018, the Transportation Security Administration's Surface Security Plan identified improvised explosive devices as key risks to energy pipelines, which "are vulnerable to terrorist attacks largely due to their stationary nature, the volatility of transported products, and [their] dispersed nature." Among these risks, according to some analysts, are the possibility of multiple, coordinated attacks with explosives on the natural gas pipeline system, which potentially could "create unprecedented challenges for restoring gas flows."

Pipeline Cybersecurity

As with any internet-enabled technology, the computer systems used to operate much of the pipeline system are vulnerable to outside manipulation. An attacker can exploit a pipeline control system in a number of ways to disrupt or damage pipelines. Such cybersecurity risks came to the fore in 2012 after reports of a series of cyber intrusions among U.S. natural gas pipeline operators. In April 2018, new cyberattacks reportedly caused the shutdown of the customer communications systems (separate from operation systems) at four of the nation's largest natural gas pipeline companies. Most recently, in January 2019, congressional testimony by the Director of National Intelligence singled out gas pipelines as critical infrastructure vulnerable to cyberattacks which could cause disruption "for days to weeks."

Pipeline and Electric Power Interdependency

Pipeline cybersecurity concerns are exacerbated by growing interdependency between the pipeline and electric power sectors. A 2017 Department of Energy (DOE) staff report highlighted the electric power sector's growing reliance upon natural gas-fired generation and, as a result, security vulnerabilities associated with pipeline gas supplies. These concerns were echoed in a June 2018 op-ed by two commissioners on the Federal Energy Regulatory Commission (FERC) who wrote, "as … natural gas has become a major part of the fuel mix, the cybersecurity threats to that supply have taken on new urgency." A November 2018 report by the PJM regional transmission organization concluded that "while there is no imminent threat," the security of generation fuel supplies, especially natural gas and fuel oil, "has become an increasing area of focus." In a February 2019 congressional hearing on electric grid security, the head of the North American Electric Reliability Corporation (NERC) testified that pipeline and electric grid interdependency "is fundamental" to security.

The Federal Pipeline Security Program

The Transportation Security Administration (TSA) within the Department of Homeland Security (DHS) administers the federal program for pipeline security. The Aviation and Transportation Security Act of 2001 (P.L. 107-71), which established TSA, authorized the agency "to issue, rescind, and revise such regulations as are necessary" to carry out its functions (§101). The Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L. 110-53) directs TSA to promulgate pipeline security regulations and carry out necessary inspection and enforcement if the agency determines that regulations are appropriate (§1557(d)). However, to date, TSA has not issued such regulations, relying instead upon industry compliance with voluntary guidelines for pipeline physical and cybersecurity. The pipeline industry maintains that regulations are unnecessary because pipeline operators have voluntarily implemented effective physical and cybersecurity programs. The 2018 GAO study identified a number of weaknesses in the TSA program, including inadequate staffing, outdated risk assessments, and uncertainty about the content and effectiveness of its security standards.

In fulfilling its responsibilities, TSA cooperates with the Department of Transportation's (DOT) Pipeline and Hazardous Materials Safety Administration (PHMSA)—the federal regulator of pipeline safety—under the terms of a 2004 memorandum of understanding (MOU) and a 2006 annex to facilitate transportation security collaboration. TSA also cooperates with DOE's recently established Office of Cybersecurity, Energy Security, and Emergency Response (CESER), whose mission includes "emergency preparedness and coordinated response to disruptions to the energy sector, including physical and cyber-attacks." TSA also collaborates with the Office of Energy Infrastructure Security at the Federal Energy Regulatory Commission—the agency which regulates the reliability and security of the bulk power electric grid.

Issues for Congress

Over the last few years, most debate about the federal pipeline security program has revolved around four principal issues. Some in Congress have suggested that TSA's current pipeline security authority and voluntary standards approach may be appropriate, but that the agency may require greater resources to more effectively carry out its mission. Others stakeholders have debated whether security standards in the pipeline sector should be mandatory—as they are in the electric power sector—especially given their growing interdependency. Still others have questioned whether any of TSA's regulatory authority over pipeline security should move to another agency, such as the DOE, DOT, or FERC, which they believe could be better positioned to execute it. Concern about the quality, specificity, and sharing of information about pipeline threats also has been an issue.

U.S. Secret Service Protection of Persons and Facilities

(Shawn Reese; March 6, 2019)

Congress has historically legislated and conducted oversight on the U.S. Secret Service (USSS) because of USSS' public mission of protecting individuals such as the President and his family, and the USSS mission of investigating financial crimes. Most recently, the 115th Congress conducted oversight on challenges facing the Service and held hearings on legislation that addressed costs associated with USSS protective detail operations and special agents' pay. These two issues remain pertinent in the 116th Congress due to recent, but failed, attacks on USSS

protectees, and the media's and public's attention on the cost the USSS incurs while protecting President Donald Trump and his family.

USSS Protection Operations and Security Breaches

In October 2018, attempted bombings targeted former President Barack Obama, former Vice President Joe Biden, and former First Lady Hillary Clinton. Prior to these attempted attacks, the media reported other USSS security breaches, including two intruders (March and October 2017) climbing the White House fence, and the USSS losing a government laptop that contained blueprints and security plans for the Trump Tower in New York City. Various security breaches during President Obama's Administration resulted in several congressional committee hearings.

Presidential safety is and has been a concern throughout the nation's history. For example, fears of kidnapping and assassination threats to Abraham Lincoln began with his journey to Washington, DC, for the inauguration in 1861. Ten Presidents have been victims of direct assaults by assassins, with four resulting in death. Since the USSS started protecting Presidents in 1906, seven assaults have occurred, with one resulting in death (President John F. Kennedy). 18 U.S.C. Section 3056(a) explicitly identifies the following individuals authorized for USSS protection:

- President, Vice President, President- and Vice President-elect;
- immediate families of those listed above;
- former Presidents, their spouses, and their children under the age of 16;
- former Vice Presidents, their spouses, and their children under the age of 16;
- visiting heads of foreign states or governments;
- distinguished foreign visitors and official U.S. representatives on special missions abroad; and
- major presidential and vice presidential candidates within 120 days of the general presidential elections, and their spouses.

USSS Protection Costs

Regardless of the location of protectees or costs associated with protective detail operations, the USSS is statutorily required to provide full-time security. Congress has reinforced this requirement in the past. In 1976, Congress required the USSS to not only secure the White House, but also the personal residences of the President and Vice President. However, the costs incurred by the USSS during the Trump Administration have generated interest and scrutiny. This includes the USSS leasing property from President Trump, and the frequency with which President Trump and his family have traveled.

Reportedly, the USSS leased property in Trump Tower in New York City. The USSS informed CRS that leasing property from a protectee is not a new requirement with the Trump Administration, but the USSS would neither confirm nor deny leasing Trump Tower property. The USSS stated that it has leased a structure in the past at former Vice President Joe Biden's personal home in Delaware to conduct security operations. The USSS will not confirm if it is still leasing this property.

Another protection cost issue other than leasing property from protectees is the overall cost of protective detail operations. One aspect of protective detail operations that has garnered attention from the media and the public is President Trump's and his family's travel. Some question whether the President and his family have traveled more than other Presidents and their families

and what, if any, impact that has on security costs. The security cost of this travel is difficult to assess, because the USSS is required to provide only annual budget justification information on "Protection of Persons and Facilities." The USSS does not provide specific costs related to individual presidential, or immediate family travel. The USSS states that it does not provide specific costs associated with protectee protection due to the information being a security concern.

Conclusion

USSS security operations and the costs associated with these operations represent consistent issues of congressional concern. USSS protectees have been—and may continue to be—targeted by assassins. Congress may wish to consider USSS protection issues within this broader context as it conducts oversight and considers funding for the ever-evolving threats to USSS protectees and the rapidly changing technology used in USSS security operations.

Protection of Executive Branch Officials

(Shawn Reese; February 19, 2019)

Due to the October 2018 attempted bombing attacks on current and former government officials (and others), there may be congressional interest in policy issues surrounding protective details for government officials. Attacks against political leaders and other public figures have been a consistent security issue in the United States. According to a 1998 U.S. Marshals Service (USMS) report, data on assassinations and assassination attempts against federal officials suggest that *elected* officials are more likely to be targeted than those holding senior *appointed* positions. Congress also may be interested due to media reports of costs or budgetary requests associated with funding security details for the heads of some departments and agencies, including the Department of Education, the Department of Labor, and the Environmental Protection Agency.

In a 2000 report, the Government Accountability Office (GAO) stated that it was able to identify only one instance when a Cabinet Secretary was physically harmed as a result of an assassination attempt. This occurred when one of the Lincoln assassination conspirators attacked then-Secretary of State William Seward in his home in 1865. Even with few attempted attacks against appointed officials, GAO reported that federal law enforcement entities have provided personal protection details (PPDs) to selected executive branch officials since at least the late 1960s. In total, GAO reported that from FY1997 through FY1999, 42 officials at 31 executive branch agencies received security protection. Personnel from 27 different agencies protected the 42 officials: personnel from their own agencies or departments protected 36 officials, and personnel from other agencies or departments, such as the U.S. Secret Service (USSS) and the USMS, protected the remaining 6 officials. This Insight provides a summary of the statutory authority for executive branch official security, a Trump Administration proposal to consolidate this security under the USMS, and issues for congressional consideration.

Statutory Authority for Protection

The USSS and the State Department are the only two agencies that have specific statutory authority to protect executive branch officials. The USSS is authorized to protect specific individuals under 18 U.S.C. §3056(a); the State Department's Diplomatic Security Service special agents are authorized to protect specific individuals under 22 U.S.C. §2709(a)(3).

In 2000, GAO reported that other agencies providing protective security details to executive branch officials cited various other legal authorities. These authorities included the Inspector General Act of 1978 (5 U.S.C., App. 3), a specific delegation of authority set forth in 7 C.F.R. §2.33(a)(2), and a 1970 memorandum from the White House Counsel to Cabinet departments.

Trump Administration Proposal

The Trump Administration proposed consolidating protective details at certain civilian executive branch agencies under the USMS to more effectively and efficiently monitor and respond to potential threats. This proposal was made in an attempt to standardize executive branch official protection in agencies that currently have USMS security details or have their own employees deputized by the USMS. This proposal would not affect any law enforcement or military agencies with explicit statutory authority to protect executive branch officials, such as the USSS or the Department of State's Diplomatic Security Service.

Threat assessments would be conducted with support from the USSS. Specifically, the Trump Administration proposed that the USMS be given the authority to manage protective security details of specified executive branch officials. These officials include the Secretaries of Education, Labor, Energy, Commerce, Veterans Affairs, Agriculture, Transportation, Housing and Urban Development, and the Interior; the Deputy Attorney General; and the Administrator of the Environmental Protection Agency. The Trump Administration proposed that Deputy U.S. Marshals would protect all of these Cabinet officials.

Currently, the USMS provides Deputy U.S. Marshals only for the Secretary of Education and the Deputy Attorney General's protective details. These two departments, however, do not have explicit statutory authority for protective details.

Potential Issues for Congress

The Administration's proposal appears to authorize the USMS to staff all protective details of executive branch officials (excluding the USSS and the Departments of State and Defense) deemed to need security, even protective security details that presently are staffed by agencies' employees. Even though the USMS implements or oversees the protection of certain executive branch officials, there appears to be no current study or research to assess the number of additional U.S. Marshals that would be needed to expand protective details to identified executive branch officials under this proposal. Additionally, the proposal does not address the funding that may be needed for USMS protection of executive branch officials. The proposal, however, does state that the Office of Management and Budget would coordinate with the Department of Justice and affected agencies on the budgetary implications.

Drug Trafficking at the Southwest Border

(Kristin Finklea; January 31, 2019)

The United States sustains a multi-billion dollar illegal drug market. An estimated 28.6 million Americans, or 10.6% of the population age 12 or older, had used illicit drugs at least once in the past month in 2016. The 2018 National Drug Threat Assessment indicates that Mexican transnational criminal organizations (TCOs) continue to dominate the U.S. drug market. They "remain the greatest criminal drug threat to the United States; no other group is currently positioned to challenge them." The Drug Enforcement Administration (DEA) indicates that these TCOs maintain and expand their influence by controlling lucrative smuggling corridors along the

Southwest border and by engaging in business alliances with other criminal networks, transnational gangs, and U.S.-based gangs.

TCOs either transport or produce and transport illicit drugs north across the U.S.-Mexico border. Traffickers move drugs through ports of entry, concealing them in passenger vehicles or comingling them with licit goods on tractor trailers. Traffickers also rely on cross-border subterranean tunnels and ultralight aircraft to smuggle drugs, as well as other transit methods such as cargo trains, passenger busses, maritime vessels, or backpackers/"mules." While drugs are the primary goods trafficked by TCOs, they also generate income from other illegal activities such as the smuggling of humans and weapons, counterfeiting and piracy, kidnapping for ransom, and extortion.

After being smuggled across the border, the drugs are distributed and sold within the United States. The illicit proceeds may then be laundered or smuggled as bulk cash back across the border. While the amount of bulk cash seized has declined over the past decade, it remains a preferred method of moving illicit proceeds—along with money or value transfer systems and trade-based money laundering. More recently, traffickers have relied on virtual currencies like Bitcoin to move money more securely.

To facilitate the distribution and local sale of drugs in the United States, Mexican drug traffickers have sometimes formed relationships with U.S. gangs. Trafficking and distribution of illicit drugs is a primary source of revenue for these U.S.-based gangs and is among the most common of their criminal activities. Gangs may work with a variety of drug trafficking organizations, and are often involved in selling multiple types of drugs.

Current domestic drug threats, fueled in part by Mexican traffickers, include opioids such as heroin, fentanyl, and diverted or counterfeit controlled prescription drugs; marijuana; methamphetamine; cocaine; and synthetic psychoactive drugs. While marijuana remains the most commonly used illicit drug, officials are increasingly concerned about the U.S. opioid epidemic. As part of this, the most recent data show an elevated level of heroin use in the United States, including elevated overdose deaths linked to heroin and other opioids, and there has been a simultaneous increase in its availability, fueled by a number of factors including increased production and trafficking of heroin by Mexican criminal networks. Increases in Mexican heroin production and its availability in the United States have been coupled with increased heroin seizures at the Southwest border. According to the DEA, the amount of heroin seized in the United States, including at the Southwest border, has generally increased over the past decade; nationwide heroin seizures reached 7,979 kg in 2017, with 3,090 kg (39%) seized at the Southwest border, up from about 2,000 kg seized at the Southwest border a decade earlier.

In addition to heroin, officials have become increasingly concerned with the trafficking of fentanyl, particularly nonpharmaceutical, illicit fentanyl. Fentanyl can be mixed with heroin and/or other drugs, sometimes without the consumer's knowledge, and has been involved in an increasing number of opioid overdoses. Nonpharmaceutical fentanyl found in the United States is manufactured in China and Mexico. It is trafficked into the United States across the Southwest border or delivered through mail couriers directly from China, or from China through Canada.

Federal law enforcement has a number of enforcement initiatives aimed at countering drug trafficking, both generally and at the Southwest border. For example, the Organized Crime Drug Enforcement Task Force (OCDETF) program targets major drug trafficking and money laundering organizations, with the intent to disrupt and dismantle them. The OCDETFs target organizations that have been identified on the Consolidated Priority Organization Targets (CPOT) List, the "most wanted" list of drug trafficking and money laundering organizations. In addition, the High Intensity Drug Trafficking Areas (HIDTA) program provides financial assistance to

federal, state, local, and tribal law enforcement agencies operating in regions of the United States that have been deemed critical drug trafficking areas. There are 29 designated HIDTAs throughout the United States and its territories, including a Southwest border HIDTA that is a partnership of the New Mexico, West Texas, South Texas, Arizona, and San Diego-Imperial HIDTAs.

Several existing strategies may also be leveraged to counter Southwest border drug trafficking. For instance, the National Southwest Border Counternarcotics Strategy (NSBCS), first launched in 2009, outlines domestic and transnational efforts to reduce the flow of illegal drugs, money, and contraband across the Southwest border. In addition, the 2011 Strategy to Combat Transnational Organized Crime provided the federal government's first broad conceptualization of transnational organized crime, highlighting it as a national security concern and outlining threats posed by TCOs—one being the expansion of drug trafficking.

The 116th Congress may consider a number of options in attempting to reduce drug trafficking from Mexico to the United States. For instance, Congress may question whether the Trump Administration will continue or alter priorities set forth by existing strategies. Policymakers may also be interested in examining various federal drug control agencies' roles in reducing Southwest border trafficking. This could involve oversight of federal law enforcement and initiatives such as the OCDETF program, as well as the Office of National Drug Control Policy (ONDCP) and its role in establishing a National Drug Control Strategy and Budget, among other efforts.

Border Security Between Ports of Entry

(Audrey Singer; February 11, 2019)

The United States' southern border with Mexico runs for approximately 2,000 miles over diverse terrain, varied population densities, and discontinuous sections of public, private, and tribal land ownership. The Department of Homeland Security (DHS) Customs and Border Protection (CBP) is primarily responsible for border security, including the construction and maintenance of tactical infrastructure, installation and monitoring of surveillance technology, and the deployment of border patrol agents to prevent unlawful entries of people and contraband into the United States (including unauthorized migrants, terrorists, firearms, narcotics, etc.). CBP's border management and control responsibilities also include facilitating legitimate travel and commerce.

Existing statute pertaining to border security confers broad authority to DHS to construct barriers along the U.S. border to deter unlawful crossings, and more specifically directs DHS to deploy fencing along "at least 700 miles" of the southern border with Mexico. The primary statute is the Illegal Immigration and Immigrant Responsibility ACT (IIRIRA) as amended by the REAL ID Act of 2005, the Secure Fence Act of 2006, and the Consolidated Appropriations Act of 2008.

On January 25, 2017, President Trump issued Executive Order 13767 "Border Security and Immigration Enforcement Improvements," which addresses, in part, the physical security of the southern border and instructed the DHS Secretary to "take all appropriate steps to immediately plan, design, and construct a physical wall along the southern border, using appropriate materials and technology to most effectively achieve complete operational control." The order did not identify the expected mileage of barriers to be constructed.

The three main dimensions of border security are tactical infrastructure, surveillance technology, and personnel.

Tactical Infrastructure. Physical barriers between ports of entry (POE) on the southern border vary in age, purpose, form, and location. GAO reports that at the end of FY2015, about one-third

of the southern border, or 654 miles, had a primary layer of fencing: approximately 350 miles designed to keep out pedestrians, and 300 miles to prevent vehicles from entering. Approximately 90% of the 654 miles of primary fencing is located in the five contiguous Border Patrol sectors located in California, Arizona, and New Mexico, while the remaining 10% is in the four eastern sectors (largely in Texas) where the Rio Grande River delineates most of the border. About 82% of primary pedestrian fencing and 75% of primary vehicle fencing are considered "modern" and were constructed between 2006 and 2011. Across 37 discontinuous miles, the primary layer is backed by a secondary layer (pedestrian) as well as an additional 14 miles of tertiary fencing (typically to delineate property lines). No new miles of primary fencing have been constructed since the 654 miles were completed in 2015, but sections of legacy fencing and breached areas have been replaced. Additional tactical infrastructure includes roads, gates, bridges, and lighting designed to support border enforcement, and to disrupt and impede illicit activity.

Surveillance Technology. To assist in the detection, identification, and apprehension of individuals illegally entering the United States between POEs, CBP also maintains border surveillance technology. Ground technology includes sensors, cameras, and radar tailored to fit specific terrain and population densities. Aerial and marine surveillance vessels, manned and unmanned, patrol inaccessible regions.

Personnel. Approximately 19,500 Border Patrol agents were stationed nationwide, with most (16,600) at the southern border in FY2017. Subject to available appropriations, Executive Order 13767 calls on CBP to take appropriate action to hire an additional 5,000 Border Patrol agents. However, CBP continues to face challenges attaining statutorily established minimum staffing levels for its Border Patrol positions despite increased recruitment and retention efforts.

Southern border security may be improved by changes to tactical infrastructure, surveillance technology, and personnel. A challenge facing policymakers is in determining the optimal mix of border security strategies given the difficulty of measuring the effectiveness of current efforts. While the number of apprehensions of illegal entrants has long been used to measure U.S. Border Patrol performance, it does not measure illegal border crossers who evade detection by the Border Patrol. When apprehensions decline, whether it is due to fewer illegal entrants getting caught or fewer attempting to enter illegally is not known. Other difficulties include measuring the contribution of any single border security component in isolation from the others, assessing the extent to which enforcement actions deter illegal crossing attempts, and evaluating ongoing enforcement efforts outside of border-specific actions and their impact on border security.

Section 1092 of the FY2017 National Defense Authorization Act (NDAA) directs the Secretary of Homeland Security to provide annual metrics on border security that are intended to help address some of the challenges of measuring the impact of border security efforts. DHS has produced baseline estimates that go beyond apprehensions statistics to measure progress towards meeting the goals contained in Executive Order 13767.

Congress, through CBP appropriations—and appropriations to its predecessor agency, the Immigration and Naturalization Service (INS)—has invested in tactical infrastructure, surveillance technology, and personnel since the 1980s. Given the changing level of detail and structure of appropriations for border infrastructure over time, it is not possible to develop a consistent history of congressional appropriations specifically for border infrastructure. However, CBP has provided the Congressional Research Service (CRS) with some historical information on how it has allocated funding for border barrier planning, construction, and operations and support. Between FY2007 and FY2018, CBP allocated just over $5.0 billion to these activities, including almost $1.4 billion specifically for border barrier construction and improvement through a new "Wall Program" activity in its FY2018 budget.

The 116th Congress is considering a mix of tactical infrastructure, including fencing, surveillance technologies, and personnel to enhance border security between U.S. POEs. Some experts have warned that the northern border may need more resources and oversight than it is currently receiving in light of potential national security risks. Other border security priorities that may be considered during the 116th Congress include improvements to existing facilities and screening and detection capacity at U.S. POEs.

National Preparedness Policy

(Shawn Reese; February 19, 2019)

The United States is threatened by a wide array of hazards, including natural disasters, acts of terrorism, viral pandemics, and man-made disasters, such as the Deepwater Horizon oil spill. The way the nation strategically prioritizes and allocates resources to prepare for all hazards can significantly influence the ultimate cost to society, both in the number of human casualties and the scope and magnitude of economic damage. As authorized in part by the Post-Katrina Emergency Reform Act of 2006 (PKEMRA; P.L. 109-295), the President, acting through the Federal Emergency Management Agency (FEMA) Administrator, is directed to create a "national preparedness goal" (NPG) and develop a "national preparedness system" (NPS) that will help "ensure the Nation's ability to prevent, respond to, recover from, and mitigate against natural disasters, acts of terrorism, and other man-made disasters" (6 U.S.C. §§743-744).

Currently, NPG and NPS implementation is guided by Presidential Policy Directive 8: National Preparedness (PPD-8), issued by then-President Barack Obama on March 30, 2011. PPD-8 rescinded the existing Homeland Security Presidential Directive 8: National Preparedness (HSPD-8), which was released and signed by then-President George W. Bush on December 17, 2003.

As directed by PPD-8, the NPS is supported by numerous strategic component policies, national planning frameworks (e.g., the National Response Framework), and federal interagency operational plans (e.g., the Protection Federal Interagency Operational Plan). In brief, the NPS and its many component policies represent the federal government's strategic vision and planning, with input from the whole community, as it relates to preparing the nation for all hazards. The NPS also establishes methods for achieving the nation's desired level of preparedness for both federal and nonfederal partners by identifying the core capabilities necessary to achieve the NPG. A *capability* is defined in law as "the ability to provide the means to accomplish one or more tasks under specific conditions and to specific performance standards. A capability may be achieved with any combination of properly planned, organized, equipped, trained, and exercised personnel that achieves the intended outcome." A *core capability* is defined in PPD-8 as a capability that is "necessary to prepare for the specific types of incidents that pose the greatest risk to the security of the Nation."

Furthermore, the NPS includes annual National Preparedness Reports that document progress made toward achieving national preparedness objectives. The reports rely heavily on self-assessment processes, called the Threat and Hazard Identification and Risk Assessment (THIRA) and Stakeholder Preparedness Review (SPR), to incorporate the perceived risks and capabilities of the whole community into the NPS. In this respect, the NPS's influence may extend to federal, state, and local budgetary decisions, the assignment of duties and responsibilities across the nation, and the creation of long-term policy objectives for disaster preparedness.

It is within the Administration's discretion to retain, revise, or replace the overarching guidance of PPD-8, and the 116th Congress may provide oversight of the NPS. Congress may have interest in overseeing a variety of factors related to the NPS, such as whether

- the NPS conforms to the objectives of Congress, as outlined in the PKEMRA statute;
- the NPS is properly informed by quantitative and qualitative data and outcome metrics, such as those gathered by the THIRA and SPR, as has been regularly recommended by the Government Accountability Office;
- federal roles and responsibilities have, in Congress's opinion, been properly assigned and resourced to execute the core capabilities needed to prevent, protect against, mitigate the effects of, respond to, and recover from the greatest risks;
- nonfederal resources and stakeholders are efficiently incorporated into NPS policies; and
- federal, state, and local government officials are allocating the appropriate amount of resources to the disaster preparedness mission relative to other homeland security missions.

Ultimately, if the NPS is determined not to fulfill the objectives of the 116th Congress, Congress could consider amending the PKEMRA statute to create new requirements, or revise existing provisions, to manage the amount of discretion afforded to the President in NPS implementation. This could mean, for example, the 116th Congress directly assigning certain preparedness responsibilities to federal agencies through authorizing legislation different than those indicated by national preparedness frameworks. As a hypothetical example, Congress could decide that certain federal agencies, such as the Department of Commerce or Housing and Urban Development, should take more or less of a role in the leadership of disaster recovery efforts following major incidents than is prescribed by the National Disaster Recovery Framework. Congress also may consider prioritizing the amount of budget authority provided to some core capabilities relative to others. As a hypothetical example, Congress may prioritize resourcing those federal programs needed to support the nation's core capability of "Screening, Search, and Detection" versus resourcing those federal programs needed to support "Fatality Management Services."

Disaster Housing Assistance

(Elizabeth M. Webster; February 26, 2019)

After the President issues an emergency or major disaster declaration under the Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act, 42 U.S.C. §§5121 et seq.), the Federal Emergency Management Agency (FEMA) may provide various temporary housing assistance programs to meet disaster survivors' needs. However, limitations on these programs may make it difficult to transition disaster survivors into permanent housing. This Insight provides an overview of the primary housing assistance programs available under the Stafford Act, and potential considerations for Congress.

Transitional Sheltering Assistance

FEMA-provided housing assistance may include short-term, emergency sheltering accommodations under Section 403 of the Stafford Act (42 U.S.C. §5170b), including the Transitional Sheltering Assistance (TSA) program, which received significant attention as it was

coming to an end for disaster survivors of Hurricane Maria from Puerto Rico. This transition process highlighted challenges to helping individuals and families obtain interim and permanent housing following a disaster.

TSA is intended to provide short-term hotel/motel accommodations to individuals and families who are unable to return to their pre-disaster primary residence because a declared disaster rendered it uninhabitable or inaccessible. The initial period of TSA assistance is 5-14 days, and it can be extended in 14-day intervals for up to 6 months from the date of the disaster declaration. However, some Hurricane Maria disaster survivors from Puerto Rico remained in the TSA program for nearly one year due to extensions of the program (including by court order). Hurricane Maria is not the only incident that has received multiple TSA program extensions; disaster survivors of Hurricanes Harvey, Irma, and Sandy also received extensions for nearly a year. Research suggests that housing-instable individuals and families may have an "increased risk of adverse mental health outcomes," which may reveal a drawback to using an emergency sheltering solution, such as TSA, to house individuals and families in hotels/motels for extended periods of time.

Individuals and Households Program

Interim housing needs may be better met through FEMA's Individuals and Households Program (IHP) under Section 408 of the Stafford Act (42 U.S.C. §5174). Financial (e.g., assistance to reimburse temporary lodging expenses and rent alternate housing accommodations) and/or direct (e.g., multi-family lease and repair and manufactured housing units (MHUs)) assistance may be available to eligible individuals and households who, as a result of a disaster, have uninsured or under-insured necessary expenses and serious needs that cannot be met through other means or forms of assistance. IHP assistance is intended to be temporary, and is generally limited to a period of 18 months from the date of the declaration, but may be extended by FEMA.

Although IHP provides various assistance options, eligibility and programmatic limitations exist on their receipt and use. For example, disaster survivors whose primary residence is determined to be habitable or who have access to adequate rent-free housing may be ineligible to receive assistance, even if they are unable to return for other reasons (e.g., lack of employment). Challenges to providing financial assistance, such as rental assistance, may include lack of available, affordable housing stock. Additionally, regulations and policies may not permit FEMA to immediately adjust rental payment rates to reflect the location where a disaster survivor has relocated. So even if housing stock is available, the difference in cost may result in the inability of some eligible applicants to secure a housing unit. Challenges to providing direct assistance, such as MHUs, may include restrictions on the placement of MHUs. Additionally, FEMA's direct lease assistance program is usually only offered if rental resources are scarce, and the area where direct lease assistance is available may be limited. Further, following a catastrophic incident additional challenges include the need to restore infrastructure, community services, and employment opportunities, which may impact where disaster survivors decide to locate following a disaster. This decision may impact the benefits for which they may be eligible.

Disaster Housing Assistance Program

Following Hurricanes Katrina and Rita, Ike and Gustav, and Sandy, FEMA executed Interagency Agreements with the U.S. Department of Housing and Urban Development (HUD) to administer the Disaster Housing Assistance Program (DHAP) in order to provide rental assistance and case management services. Although DHAP fell under Section 408 of the Stafford Act and was funded through the Disaster Relief Fund, it was not subject to some of the limitations of the IHP, and it

may have allowed families to receive more assistance for longer periods of time than they may have received under IHP. Despite being identified as a promising interim housing strategy and potential solution to the challenge of meeting long-term housing needs in the National Disaster Housing Strategy, FEMA has not implemented DHAP following more recent disasters. Most recently, in response to the Governor of Puerto Rico's request to authorize DHAP, FEMA stated DHAP would not be implemented, because FEMA and HUD "offered multiple housing solutions that are better able to meet the current housing needs of impacted survivors." FEMA also noted that the Office of Inspector General (OIG) had raised concerns about DHAP's cost effectiveness; the OIG recommended that, before FEMA activates DHAP again, it "[c]onduct a cost-benefit analysis.... "

Potential Considerations for Congress

FEMA provides temporary housing assistance to meet short-term and interim disaster housing needs; however, clearly defining the use of these programs and identifying a process to assist some disaster survivors with attaining permanent housing may be needed to comprehensively address disaster housing needs throughout all phases of recovery. Congress may request an evaluation of FEMA's capacity to adequately and cost-effectively meet the needs of disaster survivors. Congress may also evaluate the roles of government and private/nonprofit entities in providing disaster housing assistance; require FEMA to collaborate with disaster housing partners to identify and outline short, interim, and long-term disaster housing solutions; and require an update to the National Disaster Housing Strategy to reflect the roles and responsibilities of housing partners, current practices and solutions, and the findings of any such evaluations. Congress may also pursue legislative solutions, including by consolidating, eliminating, or revising existing authorities and programs, or creating new programs that address unmet needs.

The Disaster Recovery Reform Act

(Elizabeth M. Webster; February 26, 2019)

The Disaster Recovery Reform Act of 2018 (DRRA, Division D of P.L. 115-254), which became law on October 5, 2018, is the most comprehensive legislation on the Federal Emergency Management Agency's (FEMA's) disaster assistance programs since the passage of the Sandy Recovery Improvement Act of 2013 (SRIA, Division B of P.L. 113-2) and, previous to that, the Post-Katrina Emergency Management Reform Act of 2006 (PKEMRA, P.L. 109-295). The legislation focuses on improving predisaster planning and mitigation, response, and recovery, and increasing FEMA accountability. As such, it amends many sections of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act, 42 U.S.C. §§5121 et seq.). Generally, DRRA's amendments to the Stafford Act apply to major disasters and emergencies declared on or after August 1, 2017. Other new authorities apply to major disasters and emergencies declared on or after January 1, 2016.

Congress may consider tracking the implementation of DRRA's requirements, which include "more than 50 provisions that require FEMA policy or regulation changes for full implementation.... " In addition to its reporting and rulemaking requirements—many of which include 2019 deadlines—much of DRRA's implementation is at FEMA's discretion.

This Insight provides an overview of some of DRRA's broad impacts with a few significant, illustrative provisions, and potential considerations for Congress.

Potential Investments in Preparedness, Response, and Recovery

DRRA includes provisions that have the potential to improve disaster preparedness, response, and recovery, but also to increase federal spending. For example, under the revised authority under Section 203 of the Stafford Act (42 U.S.C. §5133)—Predisaster Hazard Mitigation—the President may provide financial and technical assistance by setting aside up to 6% of the estimated aggregated amount of certain federal grant assistance from the Disaster Relief Fund (DRF), including grants made pursuant to awards of Public Assistance (PA) and Individual Assistance (IA) under the Stafford Act. Previously, predisaster mitigation was funded by discretionary annual appropriations, and financial assistance was limited by the amount available in the National Predisaster Mitigation Fund, which was separate from the DRF. Post-DRRA, predisaster mitigation has the potential to have significantly higher funding through the new set-aside from the DRF, but how this will be implemented and managed by FEMA remains uncertain.

Additionally, DRRA may significantly increase the amount of financial assistance provided under Section 408 of the Stafford Act (42 U.S.C. §5174)—Federal Assistance to Individuals and Households. Prior to DRRA, an individual or household could receive up to $33,300 (FY2017; adjusted annually) in financial assistance, including both housing assistance and other needs assistance (ONA). Post-DRRA, financial assistance for repairs and replacement of housing may not exceed $34,900 (FY2019; adjusted annually), and separate from that, financial assistance for ONA may not exceed $34,900 (FY2019; adjusted annually). Financial assistance to rent alternate housing accommodations is not subject to the cap. In the past, the maximum amount of financial assistance may have resulted in applicants with significant home damage and/or other needs having little to no remaining funding available to pay for rental assistance. Changes post-DRRA may result in increased spending on temporary disaster housing assistance and ONA.

FEMA may also pilot some provisions of the DRRA, as it has done with regard to management costs incurred in the administration of the PA Program and the Hazard Mitigation Grant Program (HMGP). Following the passage of DRRA, the PA management cost reimbursement rate increased to 12% of the total grant award; 7% may be used by the grantee, and 5% by the subgrantee. Previously, PA management costs were capped at 3.34% for major disasters and 3.90% for emergency declarations. Additionally, the HMGP management cost reimbursement rate increased to 15% of the total grant award; 10% may be used by the grantee, and 5% by the subgrantee. Previously, HMGP management costs were capped at 4.89% for major disasters. In addition, prior to DRRA, there was not a pass-through requirement for subgrantees to receive a percentage of management costs.

Limitations on the Ability to Recoup Funding

A number of DRRA provisions may restrict FEMA's ability to recoup assistance, and the retroactive implementation of these provisions may be of interest to Congress. For example, FEMA may waive a debt owed by an individual or household if distributed in error by FEMA and if its collection would be inequitable, provided there was no fault on behalf of the debtor. Additionally, with regard to Section 705 of the Stafford Act (42 U.S.C. §5205)—Disaster Grant Closeout Procedures—DRRA amends the statute of limitations on FEMA's ability to recover assistance. No administrative action to recover payments may be initiated "after the date that is 3 years after the date of transmission of the final expenditure report for project completion as certified by the grantee." Prior to the passage of DRRA, the statute of limitations applied to the final expenditure report for the disaster or emergency. This is a significant change because it may take years to close all of the projects associated with a disaster. Previously, it was possible to

recoup funding from projects that may have been completed and closed years prior to FEMA's pursuit of funding because the disaster was still open.

Increased Agency Accountability and Transparency

DRRA includes reporting requirements that may influence decisionmaking regarding future disaster response and recovery. The earliest reports were due not later than 90 days after DRRA's enactment (thus a deadline of January 3, 2019). Some provisions also include briefings ahead of the reporting deadline. In addition to FEMA, other federal entities are assigned responsibilities (e.g., the Office of Inspector General for the Department of Homeland Security, which was required to initiate an audit of certain FEMA contracts by November 4, 2018).

Potential Considerations for Congress

In general, among other options, Congress may consider whether to

- evaluate if FEMA's implementation of provisions fulfills congressional intent;
- review the effectiveness and impacts of FEMA's DRRA-related regulations and policy guidance; or
- assess the effects of DRRA-related changes to federal assistance for past and future disasters.

The National Flood Insurance Program (NFIP)

(Diane P. Horn; August 14, 2019)

The National Flood Insurance Program (NFIP) is authorized by the National Flood Insurance Act of 1968 (Title XIII of P.L. 90-448, as amended, 42 U.S.C. §§4001 et seq.) and is the primary source of flood insurance coverage for residential properties in the United States. The NFIP has two main policy goals: (1) to provide access to primary flood insurance, thereby allowing for the transfer of some of the financial risk from property owners to the federal government, and (2) to mitigate and reduce the nation's comprehensive flood risk through the development and implementation of floodplain management standards. A longer-term objective of the NFIP is to reduce federal expenditure on disaster assistance after floods. The NFIP engages in many "noninsurance" activities in the public interest: it identifies and maps flood hazards, disseminates flood-risk information through flood maps, requires community land-use and building-code standards, contributes to community resilience by providing a mechanism to fund rebuilding after a flood, and offers grants and incentive programs for household- and community-level investments in flood-risk reduction.

Over 22,000 communities participate in the NFIP, with more than five million policies providing over $1.3 trillion in coverage. The program collects about $4 billion in annual revenue from policyholders' premiums. Floods are the most common natural disaster in the United States, and all 50 states, plus DC, Puerto Rico, Guam, American Samoa, the U.S. Virgin Islands, and the Northern Mariana Islands have experienced flood events since May 2018.

Structure of the NFIP

The NFIP is managed by the Federal Emergency Management Agency (FEMA) through its subcomponent, the Federal Insurance and Mitigation Administration (FIMA). Communities are not legally required to participate in the program; they participate voluntarily to obtain access to

NFIP flood insurance. Communities choosing to participate in the NFIP are required to adopt land-use and control measures with effective enforcement provisions and to regulate development in the floodplain. FEMA has set forth in federal regulations the minimum standards required for participation in the NFIP; however, these standards have the force of law only if they are adopted and enforced by a state or local government. Legal enforcement of floodplain management standards is the responsibility of participating NFIP communities, which also can elect to adopt higher standards to mitigate flood risk. The NFIP approaches the goal of reducing comprehensive flood risk primarily by requiring participating communities to collaborate with FEMA to develop and adopt flood maps called Flood Insurance Rate Maps (FIRMs). Property owners in the mapped Special Flood Hazard Area (SFHA), defined as an area with a 1% annual chance of flooding, are required to purchase flood insurance as a condition of receiving a federally backed mortgage. This mandatory purchase requirement is enforced by the lender rather than FEMA. Property owners who do not obtain flood insurance when required may find that they are not eligible for certain types of disaster assistance after a flood.

Financial Standing of the NFIP

The NFIP is funded from (1) premiums, fees, and surcharges paid by NFIP policyholders; (2) annual appropriations for flood-hazard mapping and risk analysis; (3) borrowing from the Treasury when the balance of the National Flood Insurance Fund is insufficient to pay the NFIP's obligations (e.g., insurance claims); and (4) reinsurance proceeds if NFIP losses are sufficiently large. The NFIP was not designed to retain funding to cover claims for truly extreme events; instead, the statute allows the program to borrow money from the Treasury for such events. For most of the NFIP's history, the program was able to borrow relatively small amounts from the Treasury to pay claims and then repay the loans with interest. However, this changed when Congress increased the borrowing limit to $20.775 billion to pay claims in the aftermath of the 2005 hurricane season (particularly Hurricanes Katrina, Rita, and Wilma). Congress increased the borrowing limit again in 2013, after Hurricane Sandy, to the current limit of $30.425 billion.

The 2017 hurricane season was the second-largest claims year in the NFIP's history, with approximately $10.15 billion currently paid in response to Hurricanes Harvey, Irma, and Maria. At the beginning of the 2017 hurricane season, the NFIP owed $24.6 billion. On September 22, 2017, the NFIP borrowed the remaining $5.825 billion from the Treasury to cover claims from Hurricane Harvey, reaching the NFIP's borrowing limit. On October 26, 2017, Congress canceled $16 billion of NFIP debt in order to pay claims for Hurricanes Harvey, Irma, and Maria. FEMA borrowed another $6.1 billion on November 9, 2017, bringing the debt back up to $20.525 billion. As of August 2019, the NFIP has $9.9 billion of remaining borrowing authority and has paid $952.5 million in claims for the 2018 hurricanes, Florence and Michael.

The NFIP's debt is conceptually owed by current and future participants in the NFIP, as the insurance program itself owes the debt to the Treasury and pays for accruing interest on that debt through the premium revenues of policyholders. Since 2005, the NFIP has paid $2.82 billion in principal repayments and $4.4 billion in interest to service the debt through the premiums collected on insurance policies. The October 2017 cancellation of $16 billion of NFIP debt represents the first time that NFIP debt has been canceled.

NFIP Reauthorization

Since the end of FY2017, Congress has enacted 12 short-term NFIP reauthorizations. The NFIP is currently authorized until September 30, 2019. The statute for the NFIP does not contain a comprehensive expiration, termination, or sunset provision for the whole of the program. Rather,

the NFIP has multiple different legal provisions that generally tie to the expiration of key components of the program. Unless reauthorized or amended by Congress, the following will occur on September 30, 2019: (1) the authority to provide *new* flood insurance contracts will expire; however, insurance contracts entered into before the expiration would continue until the end of their policy term and (2) the authority for the NFIP to borrow funds from the Treasury will be reduced from $30.425 billion to $1 billion.

National Flood Insurance Program (NFIP) Reauthorization and Reform

(Diane P. Horn; February 19, 2019)

NFIP Reauthorization

The National Flood Insurance Program (NFIP) is the primary source of flood insurance for residential properties in the United States, with more than 5.1 million policies providing over $1.3 trillion in coverage in over 22,000 communities. Since the end of FY2017, 10 short-term NFIP reauthorizations have been enacted, and the NFIP is currently authorized until May 31, 2019. Unless reauthorized or amended by Congress, on May 31, 2019, (1) the authority to provide *new* flood insurance contracts will expire and (2) the authority for the NFIP to borrow funds from the Treasury will be reduced from $30.425 billion to $1 billion.

A number of bills were introduced in the 115th Congress to provide longer-term reauthorization of the NFIP and numerous other changes to the program. The House passed H.R. 2874 on November 14, 2017. Three reauthorization bills were introduced in the Senate, S. 1313, S. 1368, and S. 1571; however, none of these were considered by the Senate in the 115th Congress.

Premiums and Affordability

Historically, Congress has asked the Federal Emergency Management Agency (FEMA) to set NFIP premiums that are simultaneously "risk-based" and "reasonable." Except for certain subsidies, statute directs that NFIP flood insurance rates should reflect the true flood risk to the property. Properties paying less than the full risk-based rate are determined by the date when the structure was built relative to the date of the community's Flood Insurance Rate Map (FIRM), rather than the flood risk or the policyholder's ability to pay. Congress has directed FEMA to subsidize flood insurance for properties built before the community's first FIRM (the *pre-FIRM subsidy*). When FIRMs are updated, FEMA also "grandfathers" properties at their rate from past FIRMs through a cross-subsidy. Under existing law, pre-FIRM subsidies are being phased out, whereas grandfathering is retained indefinitely.

Reforming the premium structure to reflect full risk-based rates could place the NFIP on a more financially sustainable path, risk-based price signals could give policyholders a clearer understanding of their true flood risk, and a reformed rate structure could encourage more private insurers to enter the market. However, charging risk-based premiums may mean that insurance for some properties becomes unaffordable. FEMA currently does not have the authority or funding to implement an affordability program. An NFIP-funded affordability program would require either raising flood insurance rates for NFIP policyholders or diverting resources from another existing use.

Properties with Multiple Losses

An area of controversy involves NFIP coverage of properties that have suffered multiple flood losses. One concern is the cost to the program; another is whether the NFIP should continue to insure properties that are likely to have further losses. According to FEMA, claims on repetitive loss (RL) and severe repetitive loss (SRL) properties since 1968 amount to approximately $17 billion, or approximately 30% of claims paid. Reducing the number of RL and SRL properties, through mitigation or relocation, could reduce claims and improve the NFIP's financial position. Under current statute, the NFIP cannot refuse to insure any property; however, from April 1, 2019, FEMA will introduce an SRL premium equal to 5% of the annual premium for SRL properties.

Private Flood Insurance

Private insurers play a major role in administering the NFIP through the Write-Your-Own (WYO) program, where private insurance companies are paid to issue and service NFIP policies. WYO companies take on little flood risk themselves; instead, the NFIP retains the financial risk of paying claims for these policies. Few private insurers compete with the NFIP in the primary residential flood insurance market. However, private insurer interest in providing flood coverage has increased recently, and many see private insurance as a way of transferring flood risk from the federal government to the private sector. For example, FEMA has transferred $4.322 billion of its flood risk to the capital markets through reinsurance in 2017, 2018, and 2019.

Private flood insurance may offer some potential advantages over the NFIP, including more flexible policies, broader coverage, integrated coverage with homeowners' insurance, business interruption insurance, or lower-cost coverage for some consumers. Private marketing also might increase the overall amount of flood coverage purchased. More people purchasing flood insurance, either NFIP or private, could help to reduce the amount of disaster assistance provided by the federal government. Increasing private insurance, however, may have some disadvantages compared to the NFIP. Unlike the NFIP, private coverage availability would not be guaranteed to all floodplain residents, and consumer protections could vary in different states. In addition, private sector competition might increase the financial exposure and volatility of the NFIP, as private markets likely will seek out policies that offer the greatest likelihood of profit. In the most extreme case, the private market might "cherry-pick" (i.e., adversely select) the profitable, lower-risk NFIP policies that are "overpriced" either due to cross-subsidization or imprecise rate structures. This could leave the NFIP with a higher density of actuarially unsound policies that are directly subsidized or benefit from cross-subsidization. An increase in private flood insurance policies that "depopulates" the NFIP also may undermine the NFIP's ability to generate revenue, reducing the ability or extending the time required to repay previously incurred debt.

The NFIP's role has historically been broader than just providing insurance. As currently authorized, the NFIP also encompasses social goals to provide flood insurance in flood-prone areas to those who otherwise would not be able to obtain it and to reduce the government's cost after floods. The NFIP has tried to reduce the impact of floods through flood-mapping and mitigation efforts. It is unclear how effectively the NFIP could play this broader role if private insurance became a large part of the flood marketplace. The majority of funding for flood mapping and floodplain management comes from the Federal Policy Fee (FPF), paid by all NFIP policyholders. To the extent that the private flood insurance market grows and policies move from the NFIP to private insurers, FEMA would no longer collect the FPF on those policies and less money would be available for floodplain mapping and management.

Community Disaster Loans

(Michael H. Cecire; April 24, 2019)

The Community Disaster Loan (CDL) program was developed to help local governments manage tax and other revenue shortages following a disaster. Administered by the Federal Emergency Management Agency (FEMA), CDLs provide financial liquidity to local governments through a structured loan that may be converted to grants when certain financial conditions are met. CDLs are codified in Section 417 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. §5184, as amended). Modified "non-traditional" CDL programs were developed in response to Hurricanes Rita and Katrina in 2005, and CDL-type programs for Puerto Rico and the U.S. Virgin Islands (USVI) were developed following 2017's Hurricanes Harvey, Irma, and Maria.

This Insight provides an overview of traditional and non-traditional CDLs and the policy issues they may raise in the 116th Congress, particularly with regard to CDL-type instruments developed for Puerto Rico and USVI. The CDL program may be of interest to Congress given observed increases in frequency and severity of disaster events and apparent congressional interest in oversight issues related to federal disaster response in Puerto Rico and USVI.

Overview of Traditional CDLs

CDLs were first authorized in the Disaster Relief Act of 1974 (P.L. 93-288) but are defined and established in the Stafford Act (which amended the Disaster Relief Act) to help local governments manage acute tax and other revenue loss after a disaster, which could inhibit their ability to adequately serve their communities during recovery. To qualify for a traditional CDL, an applicant must be located in a presidentially declared disaster area; show substantial loss (greater than 5%) of tax and other revenues; not be in arrears on any other previous CDL loans; and be permitted to take federal loans under their respective state law. CDLs are statutorily capped at $5 million (P.L. 106-390); and are structured around underwriting criteria that account for estimated revenue losses, the local government's annual operating budget, and a disaster's economic effects. CDLs are five-year loans, extendable to 10 years at FEMA's discretion (44 C.F.R. §206.367(c)), with interest rates determined by the Treasury Secretary. FEMA also issues guidance on how a CDL can be canceled, which involves submitting evidence of disaster-related operating deficits and associated revenue analyses to FEMA.

Overview of Non-Traditional CDLs

In special circumstances, Congress has authorized FEMA to administer non-traditional CDLs and CDL-type programs with different eligibility and technical requirements. Unlike traditional CDLs, these loans are not subject to the $5 million cap, and eligible areas are more geographically concentrated. For example, as part of the federal response to extensive economic damage caused by Hurricanes Katrina and Rita, Congress passed legislation in 2005 (P.L. 109-88) and 2006 (P.L. 109-234) to make approximately $1 billion available to support nearly $1.4 billion of non-traditional CDLs. While these non-traditional CDLs initially prohibited cancelation, subsequent 2007 legislation (P.L. 110-28) mandated that cancelation be allowed.

CDL-Type Program in Puerto Rico and USVI

Following Hurricanes Harvey, Irma, and Maria, Congress passed legislation (P.L. 115-72) providing funding for CDL-type loan instruments for Puerto Rico and USVI. This was not the

first time territories received CDLs, with USVI receiving nearly $180 million in CDL funding after Hurricanes Hugo (1989) and Marilyn (1995) prior to the $5 million cap's enactment. However, while the 2017 loan instruments were based on CDLs defined in the Stafford Act, and appropriations were made to the same fund drawn for CDLs, the resulting program was functionally different due to significant exceptions and modifications, including:

- Territorial governments were considered municipalities for the purposes of the program;
- The $5 million cap was lifted;
- Loan recipients were allowed to receive more than one loan;
- Loans could only be canceled at the discretion of the Secretary of Homeland Security in consultation with the Secretary of the Treasury; and
- The Secretary of Homeland Security, in consultation with the Secretary of the Treasury, solely determined the "terms, conditions, eligible uses, and timing and amount" of such loans.

The CDL-type instrument's statutory ambiguities related to loan cancelation and terms were further complicated by Puerto Rico's broader fiscal crisis and the existence of a federal oversight board, as established by the Puerto Rico Oversight, Management, and Economic Stability Act of 2016 (PROMESA; P.L. 114-187; see CRS Report R44532, *The Puerto Rico Oversight, Management, and Economic Stability Act (PROMESA; H.R. 5278, S. 2328)*, coordinated by D. Andrew Austin). Subsequent legislation in February 2018 (P.L. 115-123) required the Puerto Rican government to establish oversight board-approved recovery plans with monthly reports as a requirement for the CDL-type loan disbursement. Given this CDL-type instrument's statutory ambiguities, the constitutional limitations of territories, and the extent of disaster across the entirety of both territories, the CDL-type program raises potential questions of equity compared to federal disaster response to states, such as in the aftermath of Hurricanes Katrina and Rita, where CDL-type disaster assistance was more comprehensive and less restricted.

Potential Policy Issues for Congress

Should the rate and severity of disaster-related damages continue along recent trends or accelerate, traditional CDLs or their non-traditional analogues may be increasingly utilized for disaster response or recovery purposes. However, due to their relatively low funding cap and specialized nature, traditional CDLs may be inadequately suited to widespread and severe disaster events. However, non-traditional CDLs or CDL-type instruments may lack sufficiently defined disbursement and cancelation criteria, which potentially contribute to concerns over equity and utility.

With respect to Puerto Rico and USVI, Congress may seek to specify program terms and cancelation criteria to bring these instruments more in line with traditional CDLs, or the types used following Hurricanes Katrina and Rita. Considering the CDL program in broader terms, Congress may consider structuring CDLs more expansively to account for a wider universe of disaster and emergency scenarios, such as state- or executive agency-based disaster declarations, expanding or lifting the $5 million cap, or simplifying the loan forgiveness process. One potential alternative would be to restructure CDLs with automatic forgiveness thresholds based on predetermined triggering criteria. Congress could also develop disaster assistance instruments that separately address immediate governmental liquidity, disaster response, and long-term recovery needs.

Firefighter Assistance Grants

(Lennard P. Kruger; March 27, 2019)

Background

Structural firefighting—which typically refers to fighting fires in residential, commercial, and other types of buildings—is primarily the responsibility of local governments. During the 1990s, shortfalls in state and local budgets, coupled with increased responsibilities of local fire departments, led many in the fire service community to call for additional financial support from the federal government.

In response, Congress established firefighter assistance grant programs within the Federal Emergency Management Agency (FEMA) to provide additional support for local fire departments. In 2000, the 106th Congress established the Assistance to Firefighters Grant Program (AFG), which provides grants directly to local fire departments and unaffiliated Emergency Medical Services (EMS) organizations to help address a variety of equipment, vehicle, training, and other firefighter-related and EMS needs. AFG also supports fire prevention projects and firefighter health and safety research and development through the Firefighter Prevention and Safety (FP&S) grant program.

Subsequently, in 2003, the 108th Congress established the Staffing for Adequate Fire and Emergency Response (SAFER) Program, which provides grants to fund firefighter hiring by career and combination fire departments, and recruitment and retention by volunteer and combination fire departments.

Funding

Firefighter assistance grants are distributed nationwide to career, volunteer, combination, and paid-on-call fire departments serving urban, suburban, and rural areas. There is no set geographical formula for the distribution of AFG or SAFER grants. Award decisions are made by a peer panel based on the merits of the application and the needs of the community. The majority of AFG funding goes to rural (mostly volunteer) fire departments, while the majority of SAFER funding goes to urban (mostly career) fire departments. The Consolidated Appropriations Act, 2019 (P.L. 116-6) appropriated $700 million for firefighter assistance grants, consisting of $350 million for AFG and $350 million for SAFER, with funds to remain available through September 30, 2020. Dating back to the programs' establishment, Congress has appropriated a total of $8.325 billion to AFG (since FY2001), and $4.235 billion to SAFER (since FY2005).

Reauthorization

On January 3, 2018, the President signed the United States Fire Administration, AFG, and SAFER Program Reauthorization Act of 2017 (P.L. 115-98). P.L. 115-98 extended the AFG and SAFER authorization through FY2023 at a level of $750 million for each program (plus additional annual increases based on the Consumer Price Index); extended sunset provisions for AFG and SAFER through September 30, 2024; provided that the U.S. Fire Administration (USFA) may develop and make widely available an online training course on AFG and SAFER grant administration; expanded SAFER hiring grant eligibility to cover the conversion of part-time or paid-on-call firefighters to full-time firefighters; directed FEMA, acting through the Administrator of USFA, to develop and implement a grant monitoring and oversight framework

to mitigate and minimize risks of fraud, waste, abuse, and mismanagement related to the AFG and SAFER grant programs; and made various technical corrections to the AFG and SAFER statute.

Impact of Government Shutdown

Firefighter assistance grants were impacted by the partial government shutdown. For all three grant programs (AFG, SAFER, and FP&S) the application and awards process was delayed. For the 2018 round, the application windows for AFG and FP&S closed in October and December, respectively, but the processing of those applications could not move forward until the shutdown ended. The opening of the 2018 round application window for SAFER grants was also delayed, and subsequently opened on February 15, 2019. For grants already awarded (in the 2017 and previous rounds), grant recipients were unable to draw down funds during the shutdown, which may have disrupted the ability of the grantees to continue grant-funded activities, including personnel costs covered by SAFER grants. This disruption may continue after the government shutdown due to a backlog of payment requests that will need to be processed once furloughed FEMA grant personnel return to work. For additional discussion on the impact of delayed grant payments due to a government shutdown, see CRS In Focus IF11020, *Introduction to the U.S. Economy: Business Investment*.

Issues

An issue for the 116th Congress is how equitably and effectively grants are being distributed and used to protect the health and safety of the public and firefighting personnel against fire and fire-related hazards. Another issue is annual appropriations for AFG and SAFER. As is the case with many federal programs, concerns over the federal budget deficit could impact funding levels for AFG and SAFER. At the same time, firefighter assistance budgets will likely receive heightened scrutiny from the fire service community, given the local budgetary shortfalls that many fire departments may face.

Additionally, a continuing issue related to SAFER hiring grants has been whether SAFER statutory restrictions should be waived to permit grantees to use SAFER funds for retention and rehiring. Division F, Title III, Section 307 of the Consolidated Appropriations Act, 2018 states that FEMA "may" grant SAFER waiver authority. However, for the 2018 round of SAFER awards, FEMA has chosen not to exercise that authority, and thus will not provide SAFER hiring grants for retaining or rehiring firefighters. The Consolidated Appropriations Act, 2019 (P.L. 116-6) (Division A, Title III, Section 307) also includes SAFER waiver authority for the FY2019 round of SAFER awards.

Emergency Communications

(Jill C. Gallagher; January 29, 2019)

Overview

First responders and other emergency personnel use emergency communications systems to communicate with each other during day-to-day operations and large-scale disasters. Emergency communication systems are also used to enable communications between the public and response agencies. Emergency communication systems include

- 911 systems that receive calls from the public, requesting assistance or reporting an emergency, and that relay those calls to response agencies (e.g., local police and fire departments);
- land mobile radio (LMR) systems that allow police, firefighters, and emergency medical service (EMS) workers to communicate with each other during day-to-day operations and disasters;
- the First Responder Network (FirstNet), the nationwide public safety broadband network, which is currently under deployment and scheduled for completion in 2022, will enable response agencies at all levels of government to communicate via voice and data (e.g., text, videos); and
- alerting systems that notify people of emergencies and warn people of danger.

These systems often rely on different technologies that can inhibit interoperability and response. For example, 911 systems are not able to send 911 text messages to first responders in the field. State and local police and fire agencies use various radio technologies that can connect responders within their agency, but may not be interoperable with surrounding systems.

Federal, state, and local public safety agencies are investing in Internet Protocol (IP)-based technologies to improve communications, coordination, and response. The federal government has created an IP-based national alerting system that allows authorized agencies to send a single alert through multiple alerting systems. The federal government has also invested in FirstNet, a nationwide seamless, IP-based, high-speed mobile communications network that will enable public safety users to communicate via voice and data with other public safety agencies. There is also interest at all levels of government in upgrading 911 systems to next generation, IP-based systems, to enable callers to share data and to interconnect systems.

Opportunities and Challenges of New Technologies

As emergency communications systems converge toward a common IP-based platform, there are opportunities and challenges. Advancements in geo-location technologies present opportunities to find 911 callers more easily; however, integration of these technologies into legacy 911 systems is challenging. Advancements in alerting have enabled officials to send alerts to mobile phones, yet some people still rely on landline phones for communications. Interconnecting systems could improve information sharing but presents challenges in terms of privacy and security of data flowing across multiple networks.

IP-based technologies enable emergency communications systems to interconnect, creating the potential for nationwide systems. The emergence of nationwide systems may create a need for new policies that integrate these new technologies into response plans and protocols, and policies that support collaborative planning, training, and exercises across all levels of government to improve response.

Further, migration to new technologies is costly. Not all jurisdictions may be able to fund technology upgrades. Adoption of new technologies may also require upgrades to and investments in emergency communications systems and private telecommunications networks.

Issues for the 116th Congress

The 116th Congress may continue its oversight of the effectiveness of emergency communications before, during, and after natural or man-made disasters (e.g., hurricanes, wildfires), and the roles and responsibilities of federal, state, and local agencies, and private telecommunications

providers during response. Congress may also to examine the effectiveness of federal programs established to promote and support emergency communications, including

- National 9-1-1 Program administered by the National Highway and Traffic Safety Administration (NHTSA) in the U.S. Department of Transportation, which provides federal leadership and coordination in supporting and promoting optimal 911 services;
- First Responder Network Authority (FirstNet), the federal authority within the National Telecommunications and Information Administration (NTIA) in the U.S. Department of Commerce established to create the nationwide public safety broadband network;
- Integrated Public Alert and Warning System (IPAWS), the national alerting system administered by the Federal Emergency Management Agency (FEMA);
- Emergency Communications Division in the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), which is responsible for promoting interoperable and coordinated communications across all levels of government; and
- federal grant programs that fund emergency communications.

Congress may also focus on the activities of the Federal Communications Commission (FCC) Public Safety and Homeland Security Bureau (PSHSB), which administers FCC policies related to emergency communications, including rules for carriers supporting 911 services; state and local use of 911 fees; public safety spectrum; public alerts, including rules for carriers delivering wireless alerts to mobile phones; disaster management and reporting of private network outages; and restoration efforts.

U.S. National Health Security

(Sarah A. Lister, February 11, 2019)

In its quadrennial *National Health Security Strategy*, the U.S. Department of Health and Human Services (HHS) states:

> U.S. National Health Security actions protect the nation's physical and psychological health, limit economic losses, and preserve confidence in government and the national will to pursue its interests when threatened by incidents that result in serious health consequences whether natural, accidental, or deliberate.

The strategy aims to ensure the resilience of the nation's public health and health care systems against potential threats, including natural disasters and human-caused incidents, emerging and pandemic infectious diseases, acts of terrorism, and potentially catastrophic risks posed by nation-state actors.

By law, the HHS Secretary "shall lead all Federal public health and medical response to public health emergencies and incidents covered by the [*National Response Framework*]," and the HHS Assistant Secretary for Preparedness and Response (ASPR) shall "[s]erve as the principal advisor to the Secretary on all matters related to Federal public health and medical preparedness and response for public health emergencies." However, under the nation's federal system of government, state and local agencies and private entities are principally responsible for ensuring health security and responding to threats. The federal government's ability to affect national health security, through funding assistance and other policies, is relatively limited.

Figure 1. HHS Secretary's Operations Center (SOC), Activated for the Wannacry Ransomware Attack, May 2017

Source: Office of the HHS Assistant Secretary for Preparedness and Response, February 6, 2019.

Notes: The health care sector was a significant target of the cyberattack. The image shows a staff briefing on cyber threat information sharing and other efforts to protect health care infrastructure.

The nation's public health emergency management laws have expanded considerably following the terrorist attacks in 2001. Since then, a number of public health emergencies revealed both improvements in the nation's readiness, and persistent gaps. The *National Health Security Preparedness Index* (NHSPI, or the Index), a public-private partnership begun in 2013, currently assesses preparedness, using 140 measures, across all 50 states and the District of Columbia. In its latest comprehensive report, for 2017, NHSPI found overall incremental improvements over earlier years. However, the report highlighted differing preparedness levels among states, stating:

> Large differences in preparedness persisted across states, and those in the Deep South and Mountain West regions lagged significantly behind the rest of the nation. If current trends continue, the average state will require 9 more years to reach health security levels currently found in the best-prepared states.

In addition, measures of health care delivery—for example, the number of certain types of health care providers (including mental health providers) per unit of population, access to trauma centers, the extent of preparedness planning in long-term care facilities, and uptake of electronic health record systems—continued to yield the lowest scores.

The readiness of individual health care facilities and services to respond to a mass casualty incident or other public health emergency has been a persistent health security challenge. Aiming to address this, the HHS Centers for Medicare & Medicaid Services (CMS) has implemented a rule that requires 17 different types of health care facilities and service providers to meet a suite of preparedness benchmarks in order to participate in (i.e., receive payments from) the Medicare and Medicaid programs. The Emergency Preparedness (EP) Rule became effective in November 2017. Policymakers may be interested to see, in NHSPI results and through other studies, the extent to which the EP Rule yields meaningful improvements in national health system preparedness in the future.

For incidents declared by the President as major disasters or emergencies under the Robert T. Stafford Disaster Relief and Emergency Assistance Act (P.L. 93-288, as amended), public assistance is available to help federal, state, and local agencies with the costs of some public health emergency response activities, such as ensuring food and water safety. However, no federal assistance program is designed specifically to cover the uninsured costs of individual health care services that may be needed as a consequence of a disaster. There is no consensus that this should be a federal responsibility. Nonetheless, during mass casualty incidents, hospitals and health care providers may face expectations to deliver care without a clear payment source of reimbursement. Also, the response to an incident could necessitate activities that begin before Stafford Act reimbursement to HHS has been approved, or that are not eligible for reimbursement under the act. (For example, there is no precedent for a major disaster declaration under the Stafford Act for an outbreak of infectious disease, and only one declaration of emergency, for West Nile virus in 2000.) Although the HHS Secretary has authority for a no-year *Public Health Emergency Fund* (PHEF), Congress has not appropriated monies to it for many years, and no funds are currently available.

On several occasions Congress has provided supplemental appropriations to address uncompensated disaster-related health care costs and otherwise unreimbursed state and local response costs flowing from a public health emergency. These incidents include Hurricane Katrina and Hurricane Sandy, the 2009 H1N1 influenza pandemic, and the Ebola and Zika virus outbreaks. Supplemental appropriations for hurricane relief were provided for costs (such as uncompensated care) that were not reimbursed under the Stafford Act. The act was not invoked for the three infectious disease incidents, and supplemental appropriations were therefore needed to fund most aspects of the federal response to those outbreaks.

Some policymakers, concerned about the inherent uncertainty in supplemental appropriations, have proposed dedicated funding approaches for public health emergency response. Two proposals in the 115th Congress (S. 196, H.R. 3579) would have appropriated funds to the PHEF. These measures did not advance. In appropriations for FY2019 (P.L. 115-245), Congress established and appropriated $50 million (to remain available until expended) to an *Infectious Diseases Rapid Response Reserve Fund,* to be administered by the Director of the HHS Centers for Disease Control and Prevention (CDC) "to prevent, prepare for, or respond to an infectious disease emergency." The 116th Congress may choose to examine any uses of this new fund by CDC, and to consider appropriations to the PHEF, as well as other options to improve national health security preparedness.

Cybersecurity

(Chris Jaikaran; March 29, 2019)

Introduction

For policymaking purposes, *cybersecurity* can be considered the security of *cyberspace*. Taking this broad view allows policymakers to examine discrete elements of cybersecurity and determine which parts to address through the legislative process. Cyberspace, itself, includes the infrastructure necessary for the internet to work (e.g., wires, modems, and servers), the services used via the internet (e.g., web applications and websites), the devices on the network (e.g., computers and Internet-of-Things devices), and the users of those devices. Cybersecurity involves many interrelated issues, such as education; workforce management; research and development; intelligence; law enforcement; and defense.

Recent congressional activity and Member statements suggest that five specific cybersecurity topics with an intersection to homeland security may arise during the 116th Congress. This Insight first discusses the importance of risk management for cybersecurity, then introduces each of those topics: Information Sharing, Critical Infrastructure Protection and Cybersecurity, Cyber Supply Chain Risk Management, Federal Agency Oversight, and Data Protection and Privacy.

Risk Management

When computer scientists refer to cybersecurity, they are generally not talking about security as an absolute and achievable state of safety. Rather, they refer to cybersecurity as a process of risk management. Risk can be managed in four ways: it can be avoided, transferred, controlled, and accepted. To know the appropriate course of action, an organization must first understand which risks they face. Risks can be understood as the *threats* an organization faces, the *vulnerabilities* they have to their systems, and the *consequences* or impacts of a successful attack against them. Risks can be managed against systems, networks, and data. In managing those risks, managers employ an *information security* model to understand risk areas and tools to address risks. Policymakers could choose to examine these risk management factors holistically, or to consider specific elements and ways to address specific risk factors.

Policy Areas

Information Sharing

Policymakers could choose to examine information sharing as a tool that may strengthen an organization's cybersecurity. The need to maintain current awareness of the relationships between technologies and attacks is a reason that information sharing is frequently included in the cybersecurity discussion. Through information sharing, one party seeks to bolster the knowledge of its partners. Information may provide opportunities for organizations to learn from one another, reduce their vulnerability to hacking, and quickly adapt to changing conditions. Successful information sharing occurs when an organization receives information, has the capability to process it, knows how to use it, and makes a change to its practices to better secure itself. However, the advantage to sharing information is only realized when the result is a valuable change in behavior because of the information shared. Some organizations may miss critical information, lack the expertise to understand it, lack the resources to take action, or otherwise not change their behavior.

Critical Infrastructure Protection and Cybersecurity

The National Infrastructure Protection Plan directs the owners and operators of facilities under the nation's 16 critical infrastructure sectors and the sector-governing bodies to consider cybersecurity risks to their sectors. However, their ability to understand risk and to provide resources to manage risk for their sectors varies. In an effort to bolster cybersecurity risk management, policymakers could choose to direct federal agencies to provide assistance to a sector or sectors; to engage in rulemaking; or to otherwise incentivize cybersecurity activities (e.g., expediting security clearances or prioritizing federal contracting opportunities).

To assist a sector, some agencies have specific programs designed to provide information, technical assistance, or capabilities for critical infrastructure. DHS can provide assistance to all sectors. The National Institute of Standards and Technology (NIST) has published a cybersecurity framework to assist those responsible for critical infrastructure.

Cyber Supply Chain Risk Management

Recent news articles and government reports have focused attention on cyber supply chain issues. Managing risks associated with a global and complex product supply chain for information technology (IT) is known as *cyber supply chain risk management* (C-SCRM). C-SCRM refers to addressing both the risks that foreign adversaries may introduce to products and unintentional risks, such as poor quality control and vendor management. Policymakers could choose to pursue legislative options to clarify agency responsibilities relative to C-SCRM, such as increasing awareness, providing oversight, prohibiting certain companies from supplying components or services, or requiring an entity to evaluate products for cyber supply chain risks.

Federal Agency Oversight

Federal agencies collect, process, store, and transmit sensitive information such as personally identifiable information and national security information. Agencies rely on IT to use this information and requested over $17 billion in cybersecurity funding for FY2020. Yet, the Government Accountability Office (GAO) bi-annually highlights that agencies face various challenges in IT management. This is despite existing statutes, guidance, and resources agencies have to assist in managing their IT. Congress could choose to pursue investigations, hearings, or legislation to improve oversight of the government's overall IT program(s), or could focus on an individual agency's cybersecurity efforts. In pursuing this oversight, Congress may review agency spending on IT and cybersecurity, and follow up on GAO and Inspector General (IG) recommendations related to improving agency IT management.

Data Security and Privacy

The Equifax breach and multiple Facebook incidents have highlighted data security and privacy issues. While these concepts may be interrelated, and certain technologies, like encryption, can help achieve both, for policymaking and operational purposes they are distinct. Data security refers to strategies to keep out unauthorized users, while privacy refers to using data regardless of where it is stored or who accessed it. In keeping with the concept of risk management, it is important to consider "from what" one is seeking to secure their data or seek to keep it private when designing policies or strategies for security and privacy. Policymakers could choose to pursue comprehensive (such as the General Data Protection Regulation) or sectoral (such as the Health Insurance Portability and Accountability Act, HIPAA, standards) approaches to data security and privacy. In the past, the federal government has addressed these issues sectorally. But recent state and federal discussions have focused on more comprehensive approaches.

Department of Homeland Security Human Resources Management

(Barbara L. Schwemle; February 8, 2019)

Human resources management (HRM) underlies the Department of Homeland Security's (DHS) mission and performance. DHS's Chief Human Capital Officer (CHCO) "is responsible for the Department's human capital program," which is described as including such elements as "human resources policy, systems, and programs for strategic workforce planning, recruitment and hiring, pay and leave, performance management, employee development, executive resources, labor relations, work/life and safety and health."

Under Title 5, Section 1402, of the *United States Code*, a CHCO's functions include "setting the workforce development strategy" and aligning HRM with "organization mission, strategic goals, and performance outcomes." DHS's Management Directorate web page includes the CHCO position under the Under Secretary for Management (USM). The Organizational Chart and Leadership web pages do not include the position under the USM nor explain that difference. At DHS, the CHCO is a career Senior Executive Service position. The incumbent CHCO assumed the position in January 2016.

The 116th Congress may decide to conduct oversight of DHS CHCO operations—including placement, role, and functions within the department—and DHS human resources management. Such reviews could focus on the department's plans for, and performance of, HRM. These plans are set forth in a Strategic Plan and an Annual Performance Report. The latter report for FY2020 is expected to be published along with the release of the department's budget request. Congress may also examine DHS activities related to the President's Management Agenda (PMA), particularly the agenda's Cross-Agency Priority Goal (CAP) to develop the federal workforce. These topics are briefly discussed below.

Hearings, roundtables, and meetings with officials and employees could inform congressional oversight on DHS appropriations, administration, and management as they relate to HRM. Annually, on or about the anniversary of DHS's official inception, which occurred on March 1, 2003, Congress could consider conducting a review that focuses specifically on the CHCO operations and HRM policies and programs. The DHS FY2020 budget request, anticipated in March 2019, may enable Congress to conduct such a review within the context of the department's Strategic Plan, Performance Report, and PMA activities.

DHS Strategic Plan

Section 2 of the GPRA Modernization Act of 2010 (P.L. 111-352) requires agency heads to submit a strategic plan that provides, among other things, "a description of how the goals and objectives are to be achieved," including a description of the "human, capital … resources required to achieve those goals and objectives." Section 230 of the Office of Management and Budget's (OMB) Circular No. A-11 (2018), "Preparation, Submission and Execution of the Budget," stated:

> An agency's Strategic Plan should provide the context for decisions about performance goals, priorities, strategic human capital planning and budget planning. It should provide the framework for the detail published in agency Annual Performance Plans, Annual Performance Reports and on Performance.gov.

DHS published its most recent publicly available Strategic Plan, covering FY2014-FY2018, in September 2015. The plan briefly mentioned HRM. To "strengthen service delivery and manage DHS resources," the plan stated that the department would "[r]ecruit, hire, retain, and develop a highly qualified, diverse, effective, mission-focused, and resilient workforce." Specific objectives identified to accomplish this were "1) building an effective, mission-focused, diverse, and inspiring cadre of leaders; 2) recruiting a highly qualified and diverse workforce; 3) retaining an engaged workforce; and 4) solidifying a DHS culture of mission performance, adaptability, accountability, equity, and results."

To obtain an understanding of progress on the plan's HRM components to date, Congress could ask the department to document the specific framework for these four objectives and the conditions and factors related to each being fulfilled. Congress could also ask DHS to include a statement about the expected publication of an updated Strategic Plan on the Strategic Planning page of its website.

DHS Annual Performance Report

A Performance Report, required by Section 3 of P.L. 111-352, is to be published by the first Monday in February each year and cover "each program activity set forth in the budget." Among the other requirements that are specified at Title 31, Section 1115(b), of the *United States Code*, the plan must "provide a description of how the performance goals are to be achieved," including "the operation processes, training, skills and technology, and the human, capital, information, and other resources and strategies required to meet those performance goals."

DHS published its most recent Performance Report, covering FY2017-FY2019, in February 2018. The report noted that the Human Capital Operating Plan (HCOP) identifies "goals, objectives, and performance measures linked to DHS strategy" and "emphasizes management integration, accountability tracking, and the use of human capital data analysis to meet DHS mission needs." According to the department, the HCOP is used to "identify and address critical skills gaps." The Performance Report stated that Component Recruitment and Outreach Plans specify "recruitment strategies" as "a key element to sustain progress in skill gap closure."

The HCOP and the Component Recruitment and Outreach Plans do not appear to be publicly available on the department's website. Congress could suggest that the department include a link to these documents on DHS.gov to facilitate consultation and oversight about measurable results for performance goals.

President's Management Agenda

The President Donald Trump Administration describes the PMA as setting forth "a long-term vision for modernizing the Federal Government." The PMA is to be implemented through CAPs that address "critical government-wide challenges." One such CAP—led by the Office of Personnel Management, OMB, and the Department of Defense—is "Developing a Workforce for the 21st Century." It seeks a strategic human capital management framework that enables managers to "hire the best employees, remove the worst employees, and engage employees." Three CAP subgoals under this objective are "Improve Employee Performance Management and Engagement," "Reskill and Redeploy Human Capital Resources," and "Simple and Strategic Hiring."

The DHS CHCO is the leader for the third CAP subgoal, which includes strategies to reduce hiring times; "better differentiate applicants' qualifications, competencies, and experience;" and "eliminate burdensome policies and procedures."

Congressional oversight of PMA activities at DHS could focus on such matters as key initiatives, measureable results, and anticipated timelines for accomplishing subgoals.

DHS Unity of Effort

(William L. Painter; March 8, 2019)

An unresolved debate dating from the origin of the Department of Homeland Security (DHS) is the extent of department management involvement in the functioning of departmental components. Some policy experts supported a strong management function, which would replace the leadership of the components, while others supported a limited management function that allowed DHS components to function freely in their areas of expertise, much as they had before.

Once the department was established in 2003, it became clear that a small management cadre could not provide adequate coordination of policy or oversight of the department. The benefits of

coordinated action by a large organization, including setting operational and budgetary priorities, were being lost due to the lack of a capable management cadre with the capacity to manage the department's diverse missions. As its components continued to perform their missions, the department undertook efforts to establish a unified identity and way of doing business. The term "One DHS" was used to describe these initiatives under Tom Ridge, the first Secretary of DHS, and the efforts continued through secretaries Michael Chertoff and Janet Napolitano.

On April 22, 2014, Jeh Johnson, the fourth secretary of DHS, issued a memorandum to DHS leadership, entitled "Strengthening Departmental Unity of Effort." This now-widely circulated memorandum set out an agenda to reform the Department of Homeland Security's way of doing business by implementing new analytical and decisionmaking processes to develop strategy, plan, and identify joint requirements across multiple department components. These would bring component leadership together above the component level to ensure unity of effort across the department.

Secretary Johnson described it this way in a *Federal Times* interview:

> We've embarked on a unity of effort initiative that promotes greater coordination among departments, greater centralized decision-making at headquarters, a more strategic approach to our budget building process, a more strategic departmentwide approach to our acquisition strategy. It is clearly a balance. Within the Department of Homeland Security there are components that long predated the Department of Homeland Security. And so what we are not asking components to do is to all act and behave together. They are distinct cultures.... But what we are asking and expecting our component leadership to do is participate with us in a more strategic approach to promote greater efficiency in how we operate, how we conduct ourselves, particularly in our budget process and in our acquisitions.

The memorandum laid out four areas of initial focus.

1. The first was to bring together senior leaders of the department in two groups: a Senior Leaders Council to discuss "overall policy, strategy, operations and Departmental guidance," and a Deputies Management Action Group (DMAG) to "advance joint requirements development, program and budget review, acquisition reform, operational planning, and joint operations."
2. The second area was to make improvements to the departmental management processes for investments. Specifically, incorporating strategic analysis and joint requirements planning into the annual budget development process, directing the DMAG to develop and facilitate a component-driven joint requirements process, and reviewing and updating the DHS acquisition oversight framework.
3. The third was developing a stronger strategy, planning, and analytic capability within the Office of Policy.
4. The fourth was to improve coordination of cross-component operations.

Bipartisan and bicameral support for these reforms was shown in several hearings during the 113th and 114th Congresses. Both House and Senate Appropriations Committee reports have included language supportive of the department's managerial reorganization, although there has been concern expressed about keeping Congress informed about progress and consequences of reorganizations in the field.

Several of the action items included in the memorandum were completed in 2014, such as the establishment of a Cost Analysis Division in the Office of the Chief Financial Officer in May 2014. The role of this division is to ensure life-cycle cost estimates are part of major acquisition plans. DHS also completed development of a Southern Border and Approaches Campaign Plan—

a four-year strategic framework for joint operations securing the southern border of the United States.

In 2015, DHS implemented a Unity of Effort Award, presented by the Secretary, recognizing "outstanding efforts to significantly improve efficiency and effectiveness across the U.S. Department of Homeland Security," specifically noting contributions to the unity of effort initiative.

At the end of the 114th Congress, Title XIX of the FY2017 National Defense Authorization Act provided specific statutory authority to DHS for certain activities connected with the Unity of Effort initiative, including authorizing joint task forces and redefining the role of the former Office of Policy and renaming it the Office of Strategy, Policy, and Plans.

At the confirmation hearing for General John Kelly, interest in management reform and the future of Johnson's Unity of Effort initiative was apparent, with both General Kelly and some Senators praising the progress that had been made. However, Secretary Kelly's six-month tenure at the department was largely devoted to other issues. Then-Deputy Secretary Elaine Duke, after a six-month tenure as Acting Secretary, noted in early 2018 that the border security mission at DHS was one where the unity of effort initiative was maturing, as components worked together to accomplish their missions. Secretary Kirstjen Nielsen, who assumed the post in December 2017, indicated in her pre-confirmation questionnaire that she intended "to assess the effectiveness of current unity of effort programs and processes and strengthen them where needed," highlighting interest in "integrating and leveraging" capabilities and promoting joint education and training.

Congress may debate the appropriate role of departmental management at DHS, the extent of engagement Congress should have as reforms go forward, and the progress of management reforms, including whether they are having the desired effect. Congress may wish to follow up on the Secretary's priorities as outlined in her questionnaire.

Author Information

William L. Painter, Coordinator
Specialist in Homeland Security and Appropriations

Michael E. DeVine
Analyst in Intelligence and National Security

Bart Elias
Specialist in Aviation Policy

Kristin Finklea
Specialist in Domestic Security

John Frittelli
Specialist in Transportation Policy

Jill C. Gallagher
Analyst in Telecommunications Policy

Frank Gottron
Specialist in Science and Technology Policy

Diane P. Horn
Analyst in Flood Insurance and Emergency Management

Chris Jaikaran
Analyst in Cybersecurity Policy

Lennard G. Kruger
Acting Section Research Manager

Sarah A. Lister
Specialist in Public Health and Epidemiology

Daniel Morgan
Specialist in Science and Technology Policy

Paul W. Parfomak
Specialist in Energy and Infrastructure Policy

David Randall Peterman
Analyst in Transportation Policy

R. Eric Petersen
Specialist in American National Government

Shawn Reese
Analyst in Emergency Management and Homeland Security Policy

John W. Rollins
Specialist in Terrorism and National Security

Barbara L. Schwemle
Analyst in American National Government

Audrey Singer
Specialist in Immigration Policy

Elizabeth M. Webster
Analyst in Emergency Management and Disaster Recovery

Disclaimer

This document was prepared by the Congressional Research Service (CRS). CRS serves as nonpartisan shared staff to congressional committees and Members of Congress. It operates solely at the behest of and under the direction of Congress. Information in a CRS Report should not be relied upon for purposes other than public understanding of information that has been provided by CRS to Members of Congress in connection with CRS's institutional role. CRS Reports, as a work of the United States Government, are not subject to copyright protection in the United States. Any CRS Report may be reproduced and distributed in its entirety without permission from CRS. However, as a CRS Report may include copyrighted images or material from a third party, you may need to obtain the permission of the copyright holder if you wish to copy or otherwise use copyrighted material.