Selected Homeland Security Issues in the 115th Congress

William L. Painter
Specialist in Homeland Security and Appropriations

May 11, 2017

Congressional Research Service
7-5700
www.crs.gov
R44847

CRS REPORT
Prepared for Members and
Committees of Congress

Summary

In 2001, in the wake of the terrorist attacks of September 11th, "homeland security" went from being a concept discussed among a relatively small cadre of policymakers and strategic thinkers to a broadly discussed issue among policymakers, including 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) and the establishment of the Department of Homeland Security (DHS). Evolution of America's response to terrorist threats has continued under the leadership of different Administrations, Congresses, and in a shifting environment of public opinion.

DHS is currently the third-largest department in the federal government, although it does not incorporate all of the homeland security functions at the federal level, even if one constrains the definition of homeland security to the narrow field of prevention and response to domestic acts of terrorism. In policymaking terms, homeland security is a very broad and complex network of interrelated issues. For example, in its executive summary, the Quadrennial Homeland Security Review issued in 2014 delineates 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 outlines an array of homeland security issues that may come before the 115th Congress. After a brief discussion of the definitions of homeland security, the homeland security budget, and the role of homeland security actors in the intelligence community, the report divides the specific issues into five broad categories:

- Counterterrorism and Security Management;
- Border Security and Trade;
- Disaster Preparedness, Response, and Recovery;
- Cybersecurity; and
- DHS Management Issues.

Each of those areas contains a survey of topics briefly analyzed by Congressional Research Service experts. The information included only scratches the surface of most of these selected issues. More detailed information on these topics and others can be obtained by consulting the CRS reports referenced herein, or by contacting the relevant CRS expert.

Contents

Contacts

What Is Homeland Security?

There is no statutory definition of homeland security that reflects the breadth of the enterprise as currently understood. Although there is a federal Department of Homeland Security, it is neither solely dedicated to homeland security missions, nor is it the only part of the federal government with significant responsibilities in this arena.

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

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 components have historical missions that do not directly relate to conventional homeland security definitions, such as the Coast Guard's environmental and boater safety missions, and Congress has in the past debated whether FEMA and its disaster relief and recovery missions belong in the department.

Some criminal justice elements could arguably be included in a broad definition of homeland security. Issues such as the role of the military in law enforcement, monitoring and policing transfers of money, human trafficking, explosives and weapons laws, and aspects of foreign policy, trade, and economics have implications for homeland security policy.

Rather than trying to resolve the question of what should or should not be considered a part of homeland security, this report is a survey of issues that have come up in the context of homeland security policy debates. After initial discussion of the definitions of homeland security, the homeland security budget, and the role of homeland security actors in the intelligence community, the report groups the issues into five general themes:

- Counterterrorism and Security Management;
- Border Security and Trade;
- Disaster Preparedness, Response, and Recovery;
- Cybersecurity; and
- DHS Management Issues

As each topic under these themes is introduced, the author of the section is listed, along with their contact information. In many cases, a specific CRS report is highlighted as a source of more detailed information.[1]

This report is neither exhaustive nor exclusive in its scope, but representative of the broad array of issues likely to be taken up in one way or another by the 115th Congress in the coming months. The report includes many issues that were touched upon in the 114th Congress through legislation or hearings, and remain unresolved. Some specific issues or issue areas are explored from a variety of perspectives in other CRS work (e.g., issues with law enforcement, domestic policy, or

[1] In cases where an author has left CRS prior to the date of publication, only the supporting reports are mentioned in the text, while the author is listed in a footnote.

national security aspects), and the reader is encouraged to reach out to CRS directly or explore the CRS website to take full advantage of the products available to them on these matters.

While this report may be updated, it should be viewed as an introduction, not a legislative tracker. Therefore, some issues currently under debate are not included as a focal item in this report, as the state of the debate is highly dynamic (e.g., the Administration's proposed construction of a wall on the U.S.-Mexico border), and other CRS analytical products provide more current analysis than can practically be provided in a report of this breadth.

The Budget and Security

William L. Painter, Specialist in Homeland Security Policy and Appropriations (wpainter@crs.loc.gov, 7-3335)

For more information, see CRS Report R44621, *Department of Homeland Security Appropriations: FY2017*, coordinated by William L. Painter, and CRS Report R44052, *DHS Budget v. DHS Appropriations: Fact Sheet*, by William L. Painter.

From FY2003 through FY2015, according to data from the Office of Management and Budget (OMB), the entire U.S. government spent almost $807 billion (in nominal dollars) on "homeland security"—defined in law as "those activities that detect, deter, protect against, and respond to terrorist attacks occurring within the United States and its territories." Such spending peaked in FY2009 at $73.8 billion. The OMB indicated that its initial estimate of the total budget for homeland security activities for FY2016 was $71.7 billion.[2]

By comparison, the budget for the Department of Homeland Security has grown from $31.2 billion in FY2003, when it did not have its own appropriations bill, to $63.5 billion in FY2015, the last year for which we have complete budget data as of the date of publication. Roughly $36.7 billion of that amount, or 57.8%, was considered "homeland security" spending by OMB's accounting under the above definition. Some argue that the definition in law is too focused on explicit and directly attributable counterterrorism activities compared to broader theories that have been part of the national discussion, which consider immigration and border control or disaster response as a part of homeland security.

DHS Appropriations

For FY2017, the Obama Administration requested $47.3 billion in discretionary budget authority for DHS, including over $6.7 billion to pay for the costs of major disasters under the Stafford Act. Additional Overseas Contingency Operations (OCO) funding was requested by the Administration for the Coast Guard as a transfer from the U.S. Navy.

Neither the Senate bill[3] nor the House bill[4] that were reported out of their respective appropriations committees in response to that request received floor consideration.

On September 29, 2016, President Obama signed P.L. 114-223 into law, which contained a continuing resolution that funded the government at the same rate of operations as FY2016, minus 0.496% through December 9, 2016. A second continuing resolution was signed into law on

[2] Finalized budget totals for FY2016, reflecting reprogrammings and transfers, are expected with the release of the complete FY2018 budget request.

[3] S. 3001, accompanied by S.Rept. 114-264.

[4] H.R. 5634, accompanied by H.Rept. 114-668.

December 10, 2016 (P.L. 114-254), funding the government at the same rate of operations as FY2016, minus 0.1901%, through April 28, 2017. A third continuing resolution extended funding at that rate through May 5, 2017.

On March 16, 2017, the Trump Administration submitted an amendment to the FY2017 budget request. The amendment proposed $3 billion more in funding for DHS, including funding for construction of a border wall and increases in staffing for U.S. Customs and Border Protection and Immigration and Customs Enforcement that had been called for by President Trump in Executive Orders signed January 25, 2017.

On May 5, 2017, President Trump signed into law P.L. 115-31, Division F of which was the Department of Homeland Security Appropriations Act, 2017. The act included $49.3 billion in discretionary budget authority for DHS for FY2017, $1.1 billion of which was included as supplemental appropriations in response to the March request and emerging developments.

The act included a finalized reorganization of most of the structure of DHS appropriations intended to improve transparency. However, the appropriations for the U.S. Coast Guard continue to be presented in their old structure due to complications with their financial management system.

The current budget environment will likely present challenges to homeland security programs, DHS components, and the department as a whole, 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, will compete with one another for limited funding across the government and within DHS. The potential impact of the changing budget environment is discussed at various points throughout this report.

Homeland Security and the U.S. Intelligence Community

Anne Daugherty Miles, Research Fellow, Intelligence and National Security Policy (amiles@crs.loc.gov, 7-7739)

Heidi Peters, Research Librarian (hpeters@crs.loc.gov, 7-0702)

While many think of homeland security only in terms of DHS, it is a primary mission of the entire Intelligence Community (IC). In the years since 9/11, the "wall" between foreign and domestic intelligence has fallen and many efforts have been initiated to better integrate the capabilities residing in intelligence and law enforcement organizations.[5] "National intelligence" has come to mean "all intelligence," not just foreign intelligence.[6]

The many barriers between foreign and domestic intelligence that existed prior to 9/11 were intended to prevent government spying on U.S. persons and focused the IC on foreign intelligence. The tragedy of the 9/11 attacks overcame earlier concerns and led Congress and the

[5] See, for example, National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (Washington, DC: GPO, 2004), pp. 78-80, under "Legal Constraints on the FBI and 'the Wall.'" See also Jerry Berman and Lara Flint, "Commentary: Guiding lights: Intelligence Oversight and Control for the Challenge of Terrorism." *Criminal Justice Ethics* 22, no. 1 (2003): 2-58, at https://www.cdt.org/files/030300guidinglights_3.pdf. They suggest that there were numerous barriers: "There was never just one wall … there were really many walls, built between and within agencies…. Some walls were meant to protect individual rights. Others were meant to protect national security interests."

[6] P.L. 108-458, §1012. For more on "national intelligence," see CRS In Focus IF10525, *Defense Primer: National and Defense Intelligence*, by Anne Daugherty Miles.

executive branch to enact legislation, 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 DHS responsibility for fusing 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 IC.[7] New legal authorities accompanied these organizational changes.[8] At the state and local level, initiatives to improve collaboration across the federal system, such as the FBI-led Joint Terrorism Task Forces (JTTFs), have expanded—the number of JTTFs across the country grew from 34 to over 100 between 2001 and 2017—and new ones, such as DHS's National Network of Fusion Centers (NNFC), have been put in place.[9]

The "community" of U.S. government entities that perform some kind of intelligence-related activity has gradually evolved into 17 organizations/agencies that span six separate government departments and two independent agencies.[10] Two intelligence elements of DHS and one element of the FBI are most closely associated with homeland security.[11]

DHS's missions include "preventing terrorism and enhancing security; securing and managing our borders; enforcing and administering our immigration laws; strengthening cyberspace and critical infrastructure; and strengthening national preparedness and resilience to disasters."[12]

- DHS's Office of Intelligence and Analysis (OIA) provides intelligence support across the full range of DHS missions. OIA combines the unique information collected by DHS components as part of their operational activities (e.g., at airports, seaports, and the border) with foreign intelligence from the IC; law enforcement information from federal, state, local, and tribal sources; private sector data about critical infrastructure and key resources; and information from domestic open sources to develop homeland security intelligence.[13] OIA analytical products focus on a wide range of homeland security threats to include

[7] For more on the DNI position, see CRS In Focus IF10470, *The Director of National Intelligence (DNI)*, by Anne Daugherty Miles.

[8] For example, post 9/11 amendments to the Foreign Intelligence Surveillance Act of 1978 broadened the ability of federal government organizations to collect and share intelligence information domestically.

[9] Federal Bureau of Investigation, "Protecting America From Terrorist Attack: Our Joint Terrorism Task Forces," at http://www.fbi.gov/about-us/investigate/terrorism/terrorism_jttfs; U.S. Department of Homeland Security, *Fusion Centers and Joint Terrorism Task Forces*, at http://www.dhs.gov/fusion-centers-and-joint-terrorism-task-forces; and U.S. Department of Homeland Security, *National Network of Fusion Centers Fact Sheet*, at https://www.dhs.gov/national-network-fusion-centers-fact-sheet.

[10] For a brief overview of the 17 components of the IC, see CRS In Focus IF10469, *The U.S. Intelligence Community (IC)*, by Anne Daugherty Miles.

[11] For details on all 17 components of the IC see Office of the Director of National Intelligence, *U.S. National Intelligence: An Overview 2013*, at http://www.dni.gov/files/documents/USNI%202013%20Overview_web.pdf. See also CRS Report R44681, *Intelligence Community Programs, Management, and Enduring Issues*, by Anne Daugherty Miles.

[12] U.S. Department of Homeland Security, "Homeland Security Roles and Responsibilities," Appendix A in *2014 Quadrennial Homeland Security Review*, June 18, 2014, p. 83, at http://www.dhs.gov/sites/default/files/publications/2014-qhsr-final-508.pdf.

[13] For more on domestic intelligence see Greg Treverton, "Reorganizing U.S. Domestic Intelligence: Assessing the Options," *Monograph*, RAND Corporation, 2008, at http://www.rand.org/pubs/monographs/MG767.html.

foreign and domestic terrorism, border security, human trafficking, and public health.[14] 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.[15]

- The U.S. Coast Guard (USCG), made part of DHS in 2002, has intelligence elements that deal with information relating to maritime security and homeland defense. The USCG's responsibilities include protecting citizens from the sea (maritime safety), protecting America from threats delivered by the sea (maritime security), and protecting the sea itself (maritime stewardship). Its diverse mission sets and broad legal authorities allow it to fill a unique niche within the IC.[16]

The FBI functions as both an intelligence *and* law enforcement agency.[17] Immediately after the attacks of September 11, 2001, investigators highlighted a number of obstacles to information sharing among the nation's intelligence and law enforcement communities, and called for related reforms. In the decade following 9/11, a number of laws and executive orders included provisions designed to improve the FBI's counterterrorism efforts.[18] For example, the IRTPA of 2004 (P.L. 108-458) directed the FBI Director "to develop and maintain a specialized and integrated national intelligence workforce consisting of agents, analysts, linguists, and surveillance specialists who are recruited, trained, and rewarded in a manner which ensures the existence within the FBI of an institutional culture with substantial expertise in, and commitment to, the intelligence mission of the Bureau."[19]

The FBI Intelligence Branch "oversees intelligence policy and guidance." It includes the Directorate of Intelligence, "the FBI's dedicated national intelligence workforce."[20] The directorate has "clear authority and responsibility for all Bureau intelligence functions" and includes intelligence elements and personnel that reside at FBI Headquarters and in each FBI field division.[21] Such elements play a role in much of the investigative work that the FBI pursues. For example, intelligence is central to FBI efforts to thwart national security threats. Such activity is broadly managed by the FBI National Security Branch which includes:

[14] DHS, "Office of Intelligence and Analysis," at https://www.dhs.gov/office-intelligence-and-analysis.

[15] Ibid. See also Office of the Director of National Intelligence, *U.S. National Intelligence: An Overview 2013*, pp. 19-20, at http://www.dni.gov/files/documents/USNI%202013%20Overview_web.pdf.

[16] U.S. Coast Guard, *Intelligence*, Coast Guard Publication 2-0, May 2010, at https://www.uscg.mil/doctrine/CGPub/CG_Pub_2_0.pdf.

[17] For more on the FBI's role in the IC, see Joint Publication 2-01, *Joint and National Intelligence Support to Military Operations*, January 5, 2012, p. A-9.

[18] See for example USA PATRIOT Act (2001) (P.L. 107-56); USA PATRIOT Reauthorization and Improvement Act of 2005 (P.L. 109-177), and E.O. 12333, as amended by E.O.s 13284 (2003), 13355 (2004) and 13470 (2008).

[19] P.L. 108-458 §2001(c).

[20] See https://www.fbi.gov/about/leadership-and-structure/intelligence-branch.

[21] Ibid. Unlike other IC entities, the FBI is authorized to conduct HUMINT operations within the United States as part of its law enforcement duties. FBI/DI uses this authority to conduct source operations and interrogations of known or suspected terrorists, criminals, or facilitators on U.S. soil. See testimony of FBI Director Robert S. Mueller III, U.S. Congress, House Permanent Select Committee on Intelligence, *The State of Intelligence Reform 10 Years after 9/11*, hearings, 112th Cong., 1st sess., October 6, 2011, at https://www.fbi.gov/news/testimony/the-state-of-intelligence-reform-10-years-after-911.

- The Counterintelligence Division. It focuses on preventing theft of sensitive information and advanced technologies.[22]
- The Counterterrorism Division. It oversees counterterrorism investigations and the JTTFs located in FBI field divisions.[23]
- The High-Value Detainee Interrogation Group. It is a multiagency body administered by the FBI and "brings together intelligence professionals from the U.S. Intelligence Community to conduct interrogations that strengthen national security and that are consistent with the rule of law."[24]
- The Weapons of Mass Destruction Division. It helps coordinate intelligence-related efforts designed to prevent the use of chemical, biological, radiological, and nuclear weapons.[25]
- The Terrorist Screening Center. It maintains the U.S. government's consolidated watch list of known or suspected terrorists.[26]

Law enforcement information is expected to be shared with other intelligence agencies for use in all-source products.[27] In 2016 testimony to the Senate Committee on Homeland Security and Governmental Affairs, then-FBI Director James Comey commented on the importance of sharing intelligence within the broader context of the FBI's "intelligence transformation:"

> Integrating intelligence and operations is part of the broader intelligence transformation the FBI has undertaken in the last decade. We are making progress, but have more work to do. We have taken two steps to improve this integration. First, we have established an Intelligence Branch within the FBI headed by an executive assistant director (EAD). The EAD looks across the entire enterprise and drives integration. Second, we now have special agents and new intelligence analysts at the FBI Academy engaged in practical training exercises and taking core courses together. As a result, they are better prepared to work well together in the field. Our goal every day is to get better at using, collecting and sharing intelligence to better understand and defeat our adversaries.[28]

[22] See https://www.fbi.gov/about/leadership-and-structure/national-security-branch; FBI, *Intelligence National Strategy*, November 4, 2011, at https://www.fbi.gov/news/stories/2011/november/counterintelligence_110411. See also E.O. 12333 §1.3 (b) (20) (A) which directs the intelligence elements of the FBI to: (1) Collect (including through clandestine means), analyze, produce, and disseminate foreign intelligence and counterintelligence to support national and departmental missions; (2) Conduct counterintelligence activities; and (3) Conduct foreign intelligence and counterintelligence liaison relationships with intelligence, security, and law enforcement services of foreign governments or international organizations.

[23] See https://www.fbi.gov/investigate/terrorism. For more information on FBI counterterrorism investigations, see CRS Report R44521, *The Islamic State's Acolytes and the Challenges They Pose to U.S. Law Enforcement*, by Jerome P. Bjelopera; and CRS Report R41780, *The Federal Bureau of Investigation and Terrorism Investigations*, by Jerome P. Bjelopera.

[24] See https://www.fbi.gov/about/leadership-and-structure/national-security-branch/high-value-detainee-interrogation-group.

[25] See https://www.fbi.gov/investigate/wmd.

[26] See https://www.fbi.gov/about/leadership-and-structure/national-security-branch/tsc. For more information see CRS Report R44678, *The Terrorist Screening Database and Preventing Terrorist Travel*, by Jerome P. Bjelopera, Bart Elias, and Alison Siskin.

[27] "All-source" products include analysis based on information from all available sources, including those from inside and outside the intelligence community.

[28] James Comey, FBI Director, *Fifteen Years After 9/11: Threats to the Homeland*, Statement Before the Senate Committee on Homeland Security and Governmental Affairs, Washington, DC, September 27, 2016, at https://www.fbi.gov/news/testimony/fifteen-years-after-911-threats-to-the-homeland.

Selected Intelligence Community (IC) Issues with Homeland Security Implications

Domestic Surveillance

Domestic surveillance issues will likely be a concern for the 115th Congress principally because certain provisions of the Foreign Intelligence Surveillance Act (FISA) of 1978 (P.L. 95-511),[29] primarily those associated with Title VII, will sunset on December 31, 2017.

FISA provides a statutory framework regulating when government agencies may gather foreign intelligence through electronic surveillance or physical searches, capture the numbers dialed on a telephone line (pen registers) and identify the originating number of a call on a particular phone line (with trap and trace devices), or access specified business records and other tangible things. Authorization for such activities is typically obtained via a court order from the Foreign Intelligence Surveillance Court (FISC), a specialized court created to act as a neutral judicial decision maker in the context of FISA. The 9/11 attacks prompted a new look at FISA's surveillance and search provisions. Major revisions are associated with several pieces of legislation: Intelligence Authorization Act (IAA) for Fiscal Year (FY) 1999 (P.L. 105-272); USA PATRIOT Act of 2001 (P.L. 107-56),[30] IRTPA of 2004 (P.L. 108-458), Protect America Act of 2007 (P.L. 110-55), and the FISA Amendments Act of 2008 (P.L. 110-261).[31]

The USA FREEDOM Act of 2015 (P.L. 114-23), enacted during the 114th Congress, reauthorized three amendments to FISA known as the "roving" wiretap provision, the "Section 215" provision, and the "lone wolf" provisions.[32] Distinctions between the three amendments include

- Multipoint, or "roving" wiretaps allow wiretaps to follow an individual even when he or she changes the means of communication (i.e., wiretaps which may follow a target even when he or she changes phones). If it had been allowed to expire, FISA provisions would require a separate FISA Court authorization to tap each device a target uses.[33]
- "Section 215" broadened the types of records and "other tangible things" that can be made accessible to the government under FISA. If it had been allowed to expire, FISA provisions would have read as they did prior to passage of the USA PATRIOT Act, and accessible business records would have been limited to "common carrier, public accommodation facility, physical storage facility, or vehicle rental facility."[34]

[29] The original FISA legislation, P.L. 95-511 is available at http://www.gpo.gov/fdsys/pkg/STATUTE-92/pdf/STATUTE-92-Pg1783.pdf. As originally passed, FISA contained three sections and was 16 pages long.

[30] The full title of the USA PATRIOT ACT is the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001.

[31] Most of the major revisions were written in response to recommendations in the *9/11 Commission Report* and in response to the perception that the government needed to improve its collection, production and dissemination of counterterrorism-related intelligence to prevent more terrorist attacks. As a result of the amendments, FISA has grown to eight sections and is now 81 pages long. P.L. 95-511, as amended, is available at http://legcounsel.house.gov/Comps/Foreign%20Intelligence%20Surveillance%20Act%20Of%201978.pdf.

[32] The first two of these provisions were part of the USA PATRIOT Act of 2001 (P.L. 107-56) and the third was passed as part of the IRTPA of 2004 (P.L. 108-458).

[33] CRS Report R40138, *Amendments to the Foreign Intelligence Surveillance Act (FISA) Expiring on December 15, 2019*, by Edward C. Liu.

[34] Ibid.

- The "lone wolf" provision allows the government to monitor individuals acting alone and potentially engaged in international terrorism, providing that they are not citizens or permanent residents of the United States. If it had been allowed to expire, there would have been no provision for individuals acting alone.[35]

Title VII was added to the original FISA legislation pursuant to the FISA Amendments Act of 2008 (P.L. 110-261) with a sunset clause that repealed Title VII on December 31, 2012. The FISA Amendments Reauthorization Act of 2012 (P.L. 112-238) authorized a five-year extension—such that Title VII will be automatically repealed on December 31, 2017, unless the 115th Congress passes legislation to extend it.

- Section 702 permits the Attorney General and the DNI to jointly authorize targeting of persons reasonably believed to be located outside the United States in order to acquire foreign intelligence information. However, it is limited in scope. For example, it is limited to targeting *non-U.S.* persons, the targeting procedures must be reasonably designed to prevent the intentional acquisition of any communication where the sender and all intended recipients are known at the time of the acquisition to be located in the United States, and procedures must be consistent with Constitutional protections afforded by the 4th Amendment. Once authorized, such acquisitions may last for periods of up to one year.[36] If it is allowed to expire, orders in effect on December 31, 2017, would be allowed to continue through their expiration date.[37] However, no new orders under Section 702 could be issued after the sunset date.

Information Sharing and Collaboration

The "wall" between domestic and foreign intelligence has come down metaphorically, but barriers to information sharing and collaboration remain between the IC and law enforcement entities, between IC entities in the various levels of government—federal, state, local, tribal, territorial—and between the public and private sector.[38]

There are a number of efforts underway to overcome those barriers. For example, the White House-led Information Sharing and Access Interagency Policy Committee (ISA IPC) focuses on government-wide standards and architecture, security and access, associated privacy protections, and best practices.[39] DHS has developed a Critical Infrastructure Information Sharing and

[35] Ibid.

[36] For more on Section 702, see CRS Report R44457, *Surveillance of Foreigners Outside the United States Under Section 702 of the Foreign Intelligence Surveillance Act (FISA)*, by Edward C. Liu.

[37] P.L. 110-261, §404(b)(1), as amended by P.L. 112-238, §2(b).

[38] Barriers to information sharing and collaboration include different uses of information collected by various organizations (e.g., data gathered for intelligence purposes vs. evidence gathered to prosecute a criminal), access to classified materials, complications associated with information technology, differing organizational cultures, and concerns over the damage caused by leaked information. Various types of DHS, IC, and law enforcement centers exist to "fuse" or bridge the gaps between organizations at all levels of government but the system for integrating intelligence-related information is far from perfect. While the passage of the USA PATRIOT Act removed much of the statutory basis for the "wall" between law enforcement and intelligence information, making it possible to share law enforcement information with analysts in intelligence agencies, experts have observed that many obstacles remain.

[39] P.L. 108-458 established the position of Program Manager (PM) to manage the information sharing environment (ISE) and to be "responsible for information sharing across the Federal Government." Consistent with the direction and policies issued by the President, the DNI, and the Director of the Office of Management and Budget (OMB), the PM-ISE issues government-wide procedures, guidelines, instructions, and functional standards, as appropriate, for the management, development, and proper operation of the ISE. For more on this topic, see "ISE governance," at (continued...)

Collaboration Program (CISCP) that shares threat, incident and vulnerability information between government and industry across critical infrastructure sectors such as the chemical, energy, dams, and financial services sectors in order to meet its public-private cybersecurity data sharing and analytical collaboration mission.[40] The FBI partners with businesses, academic institutions, state and local law enforcement agencies, and other participants through a program called InfraGard.[41] The Department of State promotes security cooperation through its Overseas Security Advisory Council partnering with business and private sector interests worldwide.[42]

Congress may choose to explore how these information-sharing organizations, and others, are measuring progress in efforts such as CISCP. Based on those metrics, it may attempt to assess the United States' current situation in terms of information sharing and collaboration on homeland security-related issues such as cybersecurity, border security, transportation security, disaster response, drug interdiction, critical infrastructure protection, and homegrown violent extremism. As Congress reviews cases of collaboration between multiple agencies, it may examine if it is clear which agency has the lead, and whether any single organization is accountable if a collaborative arrangement fails.

Homeland Security and Research and Development

Daniel Morgan, Specialist in Science and Technology Policy (dmorgan@crs.loc.gov, 7-5849)

The Directorate of Science and Technology (S&T) has primary responsibility for establishing, administering, and coordinating DHS R&D activities. The Domestic Nuclear Detection Office (DNDO) is responsible for research and development (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 related to 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.

The Under Secretary for S&T has statutory responsibility for coordination of homeland security R&D both within DHS and across the federal government.[43] The Director of DNDO also has an

(...continued)

https://www.ise.gov/ise-governance. For more on IPCs, see Alan G. Whittaker, et al., *The National Security Policy Process: The National Security Council and Interagency System*, Industrial College of the Armed Forces, National Defense University, U.S. Department of Defense, August 15, 2011, pp. 17-18.

[40] U.S. Department of Homeland Security, *CIKR Cyber Information and Collaboration Program*, at http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2013-06/ispab_june2013_menna_ciscp_one_pager.pdf. See also DHS, "Critical Infrastructure and Key Resources Cyber Information Sharing and Collaboration Program," at https://www.us-cert.gov/sites/default/files/c3vp/CISCP_20140523.pdf; and DHS, "Critical Infrastructure Sectors," at http://www.dhs.gov/critical-infrastructure-sectors.

[41] The InfraGard National Members Alliance (INMA) is comprised of 84 separate InfraGard Member Alliances (IMAs) that represent over 37,000 technical experts nationwide. Each of the 84 IMAs is geographically linked with an FBI Field Office. See "Infra Gard: Partnership for Protection," at https://www.infragard.org/Application/General/MoreInfo.

[42] The Overseas Security Advisory Council (OSAC) was created in 1985 under the Federal Advisory Committee Act to promote security cooperation between American private sector interests worldwide and the U.S. Department of State. It currently encompasses a 34-member core Council, an Executive Office, over 140 Country Councils, and more than 3,500 constituent member organizations. For more, see "About OSAC," at https://www.osac.gov/Pages/AboutUs.aspx.

[43] 6 U.S.C. 182.

interagency coordination role with respect to nuclear detection R&D.[44] Both internal and external coordination have been long-standing congressional concerns.

Regarding internal coordination, the Government Accountability Office (GAO) concluded in 2012 that because so many components of the department are involved, it is difficult for DHS to oversee R&D department-wide.[45] 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.[46] 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.[47]

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,[48] but no such plan has ever been issued. Instead, in certain areas, the National Science and Technology Council (a White House coordinating entity) has issued R&D strategies in certain topical areas, such as biosurveillance,[49] and the S&T Directorate has developed R&D plans with individual agencies in response to certain specific threats.

Provisions regarding R&D coordination have often appeared in congressional report language accompanying homeland security appropriations bills. In the 115th Congress, they may also be included in DHS reauthorization legislation.

Counterterrorism and Security Management

The Transnational Trend of Terrorism

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

For more information, see CRS Report R41004, *Terrorism and Transnational Crime: Foreign Policy Issues for Congress*.

[44] 6 U.S.C. 592.

[45] See U.S. Government Accountability Office, *Department of Homeland Security: Oversight and Coordination of Research and Development Should Be Strengthened*, GAO-12-837, September 12, 2012, http://www.gao.gov/products/GAO-12-837.

[46] "Explanatory Statement Submitted by Mr. Rogers of Kentucky, Chairman of the House Committee on Appropriations Regarding the House Amendment to the Senate Amendment on H.R. 3547, Consolidated Appropriations Act, 2014," *Congressional Record*, vol. 160, part 9 (January 15, 2014), p. H927.

[47] See U.S. Government Accountability Office, *Department of Homeland Security: Continued Actions Needed to Strengthen Oversight and Coordination of Research and Development*, GAO-14-813T, July 31, 2014, http://www.gao.gov/products/GAO-14-813T.

[48] P.L. 107-296, Sec. 302(2); 6 U.S.C. 182(2).

[49] National Science and Technology Council, *National Biosurveillance Science and Technology Roadmap*, Washington, DC, June 2013, https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/biosurveillance_roadmap_2013.pdf.

Terrorism remains a transnational threat that entails risks to U.S. global interests emanating from and manifesting in both the international and domestic environment. Central to U.S. efforts to address transnational terrorism are actions taken to detect, deter, and defeat Al Qaeda and the Islamic State. While recognizing that numerous other terrorist groups may wish to harm U.S. global security interests, the current Administration appears to be primarily focused on addressing threats from Al Qaeda and the Islamic State, their affiliated organizations, and adherents to their violence-based philosophy. Understanding how Al Qaeda and the Islamic State continue to evolve into global entities with a diverse set of actors and capabilities is central to formulating sound strategic policy and overseeing its effective implementation.

Al Qaeda

The past few years have witnessed a continuation in terrorist actions by entities claiming some affiliation with or philosophical connection to Al Qaeda. Many of the past year's global terrorist attacks were conducted by individuals or small terrorist cells that received support ranging from resources and training to having minimal connections, if any, with the terrorist groups to which they claim allegiance. Some argue that recent U.S. counterterrorism successes may be reducing the level of terrorist threats to the nation emanating from core Al Qaeda. U.S. officials suggested that the killing of Osama bin Laden in May 2011 coupled with continuous post-9/11 global military and intelligence counterterrorism actions have significantly degraded Al Qaeda's ability to successfully launch a catastrophic terrorist attack against U.S. global interests.[50] Others suggest that Al Qaeda has changed from an organization to a philosophical movement, making it more difficult to detect and defeat.[51] Still, Al Qaeda, the organization and its affiliates, persist and have drawn the attention of the Trump Administration.

The Islamic State[52]

The Islamic State (IS, also known as the Islamic State of Iraq and the Levant, ISIL, or ISIS) is a transnational Sunni Islamist insurgent and terrorist group that has expanded its control over parts of Iraq and Syria since 2013. There is debate over the degree to which the overseas members of the Islamic State organization might represent a direct terrorist threat to U.S. facilities and personnel in the region or to the U.S. homeland or whether the more significant concern relates to how unaffiliated individuals not under the control of IS leadership might become inspired to undertake attacks.[53] The forerunners of the Islamic State were part of the insurgency against coalition forces in Iraq. In the years since the 2011 U.S. withdrawal from Iraq, the organization has expanded and contracted its presence in Iraq and broadened its reach and activities in Syria. The Islamic State has thrived in the disaffected Sunni tribal areas of eastern provinces of Syria affected by the civil war. Since 2014, IS forces have killed Syrian and Iraqi adversaries, including some civilians, often from ethnic or religious minorities, and killed hostages, including U.S. citizens. Islamic State attempts to make further gains in Iraq and Syria continue. The group's

[50] For additional information, see CRS Report R41809, *Osama bin Laden's Death: Implications and Considerations*, coordinated by John W. Rollins.

[51] Haridimos Tsoukas and Robert C. H. Chia, *Philosophy and Organizational Theory*, Research in the Sociology of Organizations, Volume 32, London, U.K., 2011, pp. 287-290.

[52] For additional information, see CRS Report R43612, *The Islamic State and U.S. Policy*, by Christopher M. Blanchard and Carla E. Humud.

[53] CRS Report R43612, *The Islamic State and U.S. Policy*, by Christopher M. Blanchard and Carla E. Humud

tactics have drawn international ire, and raised U.S. attention to Iraq's political problems and to the war in Syria.[54]

Considerations

The terrorist threat to U.S. global interests will likely remain an important issue for the Administration and the 115th Congress. Over the past few years numerous individuals were arrested in the homeland and abroad for conducting attacks and planning terrorism-related activities directed at U.S. national security interests. Many of the attacks—successful and unsuccessful—were of a transnational dimension and included a lone attacker who appears to have become radicalized over the Internet, terrorist organizations wishing to use airliners as platforms for destruction, and individuals attempting to detonate large quantities of explosives or undertaking mass shootings in symbolic areas frequented by large groups of people.

The 114th Congress undertook efforts, largely through hearings, to better understand the nature of terrorism in various geographic regions and assess the effectiveness of U.S. and partnering nations' counterterrorism efforts. Programs and policies that Congress has reviewed include public diplomacy efforts; imposition of sanctions; terrorism financing rules; the nexus between international crime, narcotics, and terrorism; and the relationship between domestic and international terrorism activities. The 115th Congress may assess the Trump Administration's counterterrorism-related strategies, policies, and programs to ascertain if additional guidance or legislation is required. Any such assessments will likely include considerations of how best to balance perceived risks to U.S. global security interests with other non-security related policy priorities.

The Islamic State in the Homeland—the Departed, Returned, and Inspired

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

For more information, see CRS Report R44521, *The Islamic State's Acolytes and the Challenges They Pose to U.S. Law Enforcement*, by Jerome P. Bjelopera

Congress continues to focus attention on the threat posed by people who have pursued terrorist activity in the homeland. It may be of value for Congress to undertake its policy discussions with a broad understanding of the contours of such terrorist plotting, as well as the general types of actions the government takes to mitigate this threat.

Since 2014, the Islamic State (IS)[55] has become the focal point for the bulk of homegrown violent jihadist terrorist plots.[56] According to CRS analysis of publicly available information, IS

[54] For additional information, see CRS Report R43612, *The Islamic State and U.S. Policy*, by Christopher M. Blanchard and Carla E. Humud.

[55] The group is also referred to as the Islamic State of Iraq and the Levant (ISIL/ISIS or the Arabic acronym *Da'esh*), among other names. For more information see CRS Report R43612, *The Islamic State and U.S. Policy*, by Christopher M. Blanchard and Carla E. Humud, and CRS Report RL33487, *Armed Conflict in Syria: Overview and U.S. Response*, coordinated by Carla E. Humud.

[56] For this report, the term "homegrown" includes American citizens, lawful permanent residents, or visitors radicalized largely within the United States. "Homegrown violent jihadist" describes homegrown individuals using Islam as an ideological and/or religious justification for their belief in the establishment of a caliphate—a jurisdiction governed by a Muslim civil and religious leader known as a caliph—via violent means. Such violence can be perpetrated within the (continued...)

supporters have accounted for 80 of the approximately 91 homegrown violent jihadist plots between 2014 and February 2017. This includes instances in which people in the United States wanted to travel to Syria to fight with extremist groups in the nation's civil war as well as plots to strike domestic targets. These plots can be broken into three rough categories based on the courses of action that plotters[57] pursued as they attempted to support the terrorist group. The first two categories focus on foreign fighters,[58] the last on people who will not or have not traveled to train or fight overseas, but are willing to do harm in the United States:

- ***The Departed***—American foreign fighters who plan to leave or have left the United States to fight for the Islamic State. This group includes suspects scheming to travel but who are caught before they arrive in IS territory.
- ***The Returned***—American foreign fighters who trained with or fought in the ranks of the Islamic State and return to the United States, where they can potentially plan and execute attacks at home.[59]
- ***The Inspired***—Americans lured—in part—by IS propaganda to participate in terrorist plots within the United States.

The desire to become a foreign fighter (captured in either the departed or the returned category) played a role in 47 of the 80 IS-related plots. Almost all of the 47 had people either *departing* the United States for Syria or considering such a trip. Three of the 47 cases involved investigations of people who had returned from the conflict zone.[60] In 37 cases since the start of 2014, people *inspired* by the terrorist group's propaganda considered striking targets in the United States.[61] IS has tried to inspire attacks via its propaganda. For example, in May 2016, the group issued an audio recording, particularly encouraging American and European sympathizers to commit attacks in their home countries during the holy month of Ramadan (early June to early July).[62]

(...continued)

United States or abroad. The term homegrown violent jihadist includes

- People described by U.S. intelligence and law enforcement agencies as *homegrown violent extremists*—individuals operating in the United States who are inspired by foreign terrorist organizations but do not receive direction or assistance from such groups.
- Homegrown individuals who receive direction or assistance from foreign terrorist organizations.

[57] The 80 plots have involved more than 130 individuals in total, and this estimate includes indicted co-conspirators in criminal cases; people who died either in attacks or as foreign fighters; and instances in which some biographical identifiers exist for the individuals centrally involved in plotting. Unindicted co-conspirators, cooperating informants, and undercover law enforcement personnel are not counted.

[58] For the purposes of this report, foreign fighters are U.S. citizens and noncitizens who radicalized in the United States and plotted to or traveled abroad to join a foreign terrorist group. "Plots" include schemes by homegrown individuals or groups to either join terrorist organizations abroad (become foreign fighters) or to commit violent attacks at home or abroad. "Attacks" involve ideologically driven physical violence committed by terrorists. To qualify as an attack, the violence has to harm a person or people in the United States or those targeted as Americans abroad. Plots and attacks were dated according to when they became publicly known generally via government press releases, publicly released court documents, or news reporting.

[59] This group does not include people who left the United States but failed to join up with a terrorist group. Such individuals are among "the departed."

[60] These three plots apparently did not include viable schemes to strike domestic targets after the plotters returned to the United States.

[61] Four plots exhibited both departed and inspired qualities.

[62] Paul Cruickshank, "Orlando Shooting Follows ISIS Call for U.S. Ramadan Attacks," *CNN*, June 13, 2016; Maher Chmaytelli, Stephen Kalin, and Ali Abdelaty, "Islamic State Calls for Attacks on the West During Ramadan in Audio Message," *Reuters*, May 22, 2016; U.S. Government Open Source Enterprise (OSE) Report TRO2016052227212358, "ISIL Spokesman Urges 'Soldiers', ISIL 'Supporters' to Target 'Civilians' During Ramadan," Twitter in English, (continued...)

The January 2016 issue of *Dābiq*, the Islamic State's English language magazine, praised the married couple reportedly involved in the San Bernardino shooting in December 2015.[63]

Beyond the Departed, Returned, and Inspired

Aside from the three categories based on the courses of action that IS supporters follow, at least two other sorts of IS foreign fighters pose some threat to U.S. interests.

- ***The Lost—****unidentified* Americans who fight in the ranks of the Islamic State. Such individuals may come home after fighting abroad and remain unknown to U.S. law enforcement. Some American IS fighters will never book a trip back to the United States. (The post 9/11 record of U.S. counterterrorism investigations suggests this prospect. None of the Americans who have fought for al-Shabaab, a terrorist group based in Somalia, are known to have come home to plot attacks.) Finally, some American IS supporters will perish abroad.
- ***The Others—***foreign IS adherents who radicalize in and originate from places outside of the United States or non-American foreign fighters active in the ranks of the Islamic State. These persons could try to enter the United States from abroad.

Preempting and Monitoring Potential Terrorists

Preemption and monitoring of possible IS terrorist activity by U.S. law enforcement can be broadly described in terms of interdiction, investigation, and countering violent extremism in the United States.

Interdiction

In this sphere, interdiction activities involve—among other things—stopping a suspected terrorist from entering the United States. For example, within the Department of Homeland Security (DHS), components such as Customs and Border Protection (CBP) draw on information from the federal government's consolidated terrorist watchlist as they engage in intelligence-driven screening to mitigate the risk posed by travelers destined for the United States.[64] The federal government has also coordinated with other nations regarding identifying and interdicting foreign fighters.[65] One of the known efforts targeting foreign fighters pursued by DHS involves enhancements to the Electronic System for Travel Authorization (ESTA) used by CBP to vet

(...continued)

Arabic, May 21, 2016.

[63] Tom Winter and Robert Windrem, "New Issue of ISIS Magazine Dabiq Applauds San Bernardino Carnage," *NBC News*, January 19, 2016.

[64] In 2012, Customs and Border Protection (CBP) described commercial air travel as "the primary target of terrorist organizations seeking to attack the homeland or move operatives into the United States.... " See Kevin McAleenan, then Assistant Commissioner, U.S. Customs and Border Protection, Office of Field Operations, written statement for a House Committee on Homeland Security, Subcommittee on Border and Maritime Security hearing, "Eleven Years Later: Preventing Terrorists from Coming to America," September 11, 2012. For more on the U.S. watchlisting regimen, see CRS Report R44678, *The Terrorist Screening Database and Preventing Terrorist Travel*, by Jerome P. Bjelopera, Bart Elias, and Alison Siskin.

[65] For example see Department of Homeland Security, press release, "Statement by Secretary Johnson on the United Kingdom's Decision to Raise Their Threat Level," August 29, 2014.

prospective travelers from visa waiver countries "to determine if they pose a law enforcement or security risk before they board aircraft destined for the United States."[66]

In early 2017, the Trump Administration pursued additional broader measures it believed would thwart terrorist travel. In March 2017, the administration revised its January 27, 2017, Executive Order 13769, "Protecting the Nation from Foreign Terrorist Entry into the United States." Effective on March 16, 2017, the revision imposed a 90-day ban on the entry into the United States of certain aliens from Iran, Libya, Somalia, Sudan, Syria, and Yemen.[67] The executive order also suspended the United States Refugee Admissions Program for 120 days and lowered the number of refugees accepted annually from 110,000 to 50,000.[68]

Investigation

Discussion of counterterrorism investigation activities largely focuses on Joint Terrorism Task Forces (JTTFs) led by the Federal Bureau of Investigation (FBI) and supported by local, state, and federal agencies—including DHS.[69] The task forces fill the chief role in coordinating federal counterterrorism cases across the United States, bringing together federal, state, and local participants in the process. JTTFs have been involved in stopping individuals trying to leave the United States to fight with the Islamic State as well as investigating people who have returned from the conflict zone. Beyond U.S. borders, the FBI has legal attachés around the world that coordinate with foreign law enforcement partners to fight terrorist activity. Additionally, the Department of Justice (DOJ) has worked to expand its presence in countries that serve as transit points for foreign fighters.[70]

Interceding With People on the Cusp of Violent Radicalization

The Obama Administration created a program focused on "proactive actions to counter efforts by extremists to recruit, radicalize, and mobilize followers to violence."[71] The program—dubbed countering violent extremism (CVE)—reputedly covered potentially violent extremists acting from a variety of ideological perspectives (such as homegrown jihadists and white supremacists). It did not involve intelligence gathering or investigative work tied to criminal prosecutions. CVE

[66] For details see CBP Press Release, "Strengthening Security of the VWP through Enhancements to ESTA." For background see CRS Report RL32221, *Visa Waiver Program*, by Alison Siskin. See also Tom Warrick, Deputy Assistant Secretary for Counterterrorism Policy, Department of Homeland Security, written statement for a House Committee on Foreign Affairs joint subcommittee hearing, "ISIS and the Threat from Foreign Fighters," December 2, 2014; Jeh C. Johnson, (then) Secretary, Department of Homeland Security, written statement for a House Homeland Security Committee hearing, "Worldwide Threats to the Homeland," September 17, 2014.

[67] This includes most aliens from the six countries who either lacked a valid visa as of January 27, 2017, or whose visas expired after January 27, 2017.

[68] White House, "Protecting the Nation from Foreign Terrorist Entry Into the United States," March 6, 2017, https://www.whitehouse.gov/the-press-office/2017/03/06/executive-order-protecting-nation-foreign-terrorist-entry-united-states. See also the original order White House, Executive Order 13769, "Protecting the Nation from Foreign Terrorist Entry Into the United States," January 27, 2017, https://www.whitehouse.gov/the-press-office/2017/01/27/executive-order-protecting-nation-foreign-terrorist-entry-united-states.

[69] See http://www.fbi.gov/about-us/investigate/terrorism/terrorism_jttfs.

[70] Tal Kopan, "Holder: DOJ Expanding International Capacity to Stem Foreign Fighters," *Politico*, November 13, 2014. In September 2014, DOJ noted that one of its components, Interpol Washington, developed a program dedicated to thwarting foreign fighters. DOJ Press Release, "Interpol Washington Spearheads Foreign Terrorist Fighter Program, Serves as Catalyst for Global Information Sharing Network," September 24, 2014.

[71] White House, "Strategic Implementation Plan for Empowering Local Partners to Prevent Violent Extremism in the United States," October 2016, p. 2.

emphasized tackling the conditions and factors driving recruitment and radicalization by violent extremists—people who promoted political goals by supporting or committing ideologically motivated violence.[72] At DHS, the program largely involved community engagement and partnership efforts.[73] It appears that much of CVE addressed people who were not breaking the law but may have been on the path toward breaking the law by becoming violent extremists (e.g., terrorists).[74] It is unclear what the Trump Administration plans to do with this program, but media outlets have reported the Administration is interested in focusing it exclusively on homegrown violent jihadists.[75]

Medical Countermeasures to Chemical, Biological, Radiological, and Nuclear Terrorism

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

Following the 2001 anthrax attacks, the federal government created several programs to support the research, development, and procurement of new medical countermeasures against chemical, biological, radiological, and nuclear (CBRN) threats. Despite these efforts, many of the CBRN threats that the government deems likely to pose the highest risk lack available countermeasures. The 115th Congress may consider the effectiveness of the federal efforts and whether current programs should be continued, modified, or ended, and whether new programs should be established.

The research, development, and procurement of new CBRN medical countermeasures for civilian use involves a complex multi-agency process, largely within the Department of Health and Human Services. The Department of Homeland Security provides risk analysis to inform countermeasure prioritization. Recent Congresses have provided HHS new authorities and modified existing authorities to improve the performance, efficiency, and transparency of the multiagency process. However, some key issues remain unresolved, including those related to appropriations, interagency coordination, and countermeasure prioritization. In addition to determining the appropriate amount of funding, Congress may decide whether to return to funding a key procurement program, Project BioShield, through a multiyear advance appropriation. Policymakers may consider whether the legislative changes to planning and transparency requirements have sufficiently enhanced coordination of the multiagency countermeasure development enterprise and congressional oversight. Additionally, Congress may consider whether the current prioritization process appropriately balances effort between threats that have some available FDA-approved countermeasures, such as anthrax and smallpox, and threats which lack any such countermeasure, such as Ebola.

Chemical Facilities Security

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

[72] Ibid, pp. 1-2.

[73] For more information on such activity at DHS, see https://www.dhs.gov/countering-violent-extremism.

[74] For more information on the origins of the program see CRS Report R42553, *Countering Violent Extremism in the United States*.

[75] Julia Edwards Ainsley, Dustin Volz and Kristina Cooke, "Exclusive: Trump to Focus Counter-Extremism Program Solely on Islam—Sources," *Reuters*, February 2, 2017.

Congress authorized DHS to regulate security at chemical facilities through P.L. 113-254, the Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014. This act repealed the prior statutory authority that had been granted in the Homeland Security Appropriations Act, 2007 (P.L. 109-295, §550). The new authority expires in December 2018. As the termination date approaches, the 115th Congress will likely consider whether the authority should be reauthorized, modified, or allowed to expire.

Congress will likely consider whether the DHS Chemical Facility Anti-Terrorism Standards program (CFATS) and associated regulations appropriately balance homeland security and stakeholder needs. Congress may also consider how well DHS has implemented the program and whether the implementation is aligned with current congressional intent.

In considering whether to reauthorize CFATS, Congress may reconsider previously raised issues. The Obama Administration and some stakeholders determined that existing regulatory exemptions, such as for community water systems and wastewater treatment facilities, pose potential risks.[76] Environmental and "right-to-know" groups additionally advocate that Congress include requirements for facilities to adopt or identify "inherently safer technologies" and widely disseminate security-related information to first responders and employees.[77] The regulated industry generally opposes granting DHS the ability to require implementation of inherently safer technologies or other specific security measures. Industry stakeholders question the maturity and applicability of the inherently safer technology concept as a security measure and cite the need to tailor security approaches for each facility. The Obama Administration also identified the broad dissemination of chemical security-related information as a potential security concern. However, following the 2013 explosion of the West Fertilizer Company in West, TX, DHS discovered that information about that facility's chemical inventory had not been effectively shared between federal agencies. This led to reconsideration of existing information-sharing policies and Executive Order 13650, "Improving Chemical Facility Safety and Security."[78] Additionally, if Congress decides to reauthorize the program, then it may consider whether to make CFATS permanent or to include another expiration provision.

Electric Grid Physical Security

Paul Parfomak, Specialist in Energy Policy, Resources, Science and Industry Division (pparfomak@crs.loc.gov, 7-0030)

For more information, see CRS Report R43604, *Physical Security of the U.S. Power Grid: High-Voltage Transformer Substations*

The electric utility industry operates as an integrated system of generation, transmission, and distribution facilities to deliver electric power to consumers. In the United States, this system has over 9,000 electric generating units connected to over 200,000 miles of high-voltage transmission lines rated at 230 kilovolts (kV)[79] or greater strung between large towers.[80] This network is

[76] Oral testimony of Rand Beers, Under Secretary, National Protection and Programs Directorate, Department of Homeland Security, before the House Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, February 11, 2011.

[77] Department of Homeland Security, "Chemical Facility Anti-Terrorism Standards; Final Rule," 72 *Federal Register* 17718, April 9, 2007.

[78] Executive Order 13650, "Improving Chemical Facility Safety and Security," 78 *Federal Register* 48029, August 1, 2013.

[79] 1 kV=1,000 volts.

[80] North American Electric Reliability Corporation, "Understanding the Grid," fact sheet, August 2013, (continued...)

interspersed with hundreds of large electric power transformers whose function is to adjust electric voltage as needed to move power across the network. High voltage (HV) transformer units make up less than 3% of transformers in U.S. power substations, but they carry 60%-70% of the nation's electricity.[81] Because they serve as vital transmission network nodes and carry bulk volumes of electricity, HV transformers are critical elements of the nation's electric power grid.

The various parts of the electric power system are all vulnerable to failure due to natural or manmade events. However, HV transformers are considered by many experts to be among the most vulnerable to intentional damage from malicious acts.[82] Security analysts have long asserted that a coordinated and simultaneous attack on multiple HV transformers could have severe implications for reliable electric service over a large geographic area, crippling its electricity network and causing widespread, extended blackouts.[83] Such an event could have severe electric reliability consequences, demonstrated in recent grid security exercise, as well as serious economic and social consequences.[84] A handful of recent physical attacks on individual transformer substation—most notably a 2013 attack on an HV transformer substation in Metcalf, CA—did not cause widespread blackouts, but did highlight the physical vulnerability of HV transformer substations and drew the attention of both the media and federal officials to the utility industry's substation security efforts.[85]

Over the last decade or so the electric utility industry and government agencies have engaged in a number of initiatives to secure HV transformers from physical attack and to improve recovery in the event of a successful attack. These initiatives include coordination and information sharing, spare equipment programs, and grid security exercises, among other measures. Grid security guidelines or standards have been developed to address the physical security of the grid since at least 2002, including standards promulgated by the North American Electric Reliability Corporation (NERC) as voluntary best practices.

In November 2014, following the Metcalf attack, the Federal Energy Regulatory Commission (FERC) approved a new mandatory Physical Security Reliability Standard (CIP-014-1) proposed by NERC "to address physical security risks and vulnerabilities related to the reliable operation" of the power grid by performing risk assessments to identify their critical facilities, evaluate potential threats and vulnerabilities, and implement security plans to protect against attacks.[86] As

(...continued)

http://www.nerc.com/AboutNERC/Documents/Understanding%20the%20Grid%20AUG13.pdf. There is no industry consensus as to what voltage rating constitutes "high voltage." This report uses 230 kV as the high voltage threshold, but other studies may use a different one. See, for example: U.S. Department of Energy, *Large Power Transformers and the U.S. Electric Grid*, April 2014, p. 4.

[81] C. Newton, "The Future of Large Power Transformers," *Transmission & Distribution World*, September 1, 1997; William Loomis, "Super-Grid Transformer Defense: Risk of Destruction and Defense Strategies," Presentation to NERC Critical Infrastructure Working Group, Lake Buena Vista, FL, December 10-11, 2001.

[82] U.S. Department of Energy, *Energy Transmission, Storage, and Distribution Infrastructure*, April 2015, p. S-11.

[83] ICF, Assessment of Large Power Transformer Risk Mitigation Strategies, prepared for the U.S. Department of Energy, October 2016, p. 7.

[84] North American Electric Reliability Corporation (NERC), *Grid Security Exercise (GridEx II): After-Action Report*, March 2014, p.15; Matthew L. Wald, "Attack Ravages Power Grid. (Just a Test.)," *New York Times*, November 14, 2013.

[85] *RTO Insider*, "Substation Saboteurs 'No Amateurs,'" April 2, 2014, http://www.rtoinsider.com/pjm-grid2020-1113-03/; Chelsea J. Carter, "Arkansas Man Charged in Connection with Power Grid Sabotage," CNN, October 12, 2013; Max Brantley, "FBI Reports Three Attacks on Power Grid in Lonoke County," *Arkansas Times*, October 7, 2013; Rebecca Smith, "U.S. Risks National Blackout From Small-Scale Attack," *Wall Street Journal*, March 12, 2014.

[86] Federal Energy Regulatory Commission, *Physical Security Reliability Standard*, Docket No. RM14-15-000; Order (continued...)

of December 2016, NERC had received initial risk assessments and security plans from transmission owners and operators subject to the standard and was in discussions with FERC officials about how best to audit them.[87] While NERC's physical security standard was viewed by many as an important step in improving grid security, some policymakers have advocated additional measures to facilitate grid recovery in an emergency. For example, a 2015 report by the (DOE) also recommended a DOE-led effort to develop a critical HV transformer reserve as a source of emergency spares in the event of natural disaster or physical attack.[88]

The 114th Congress included provisions in the Fixing America's Surface Transportation (FAST) Act (P.L. 114-94), which became law on December 4, 2015, to facilitate recovery during electric grid emergencies due to physical damage and other causes. The act provides the Secretary of Energy additional authority to order emergency measures to protect or restore the reliability of critical electric infrastructure during a grid security emergency (§1104). The act also requires the Secretary of Energy to submit to Congress a plan for a Strategic Transformer Reserve (§1105). The reserve would store in strategic locations spare large power transformers to temporarily replace critical large power transformers damaged by intentional attack or destructive natural events. This section would authorize the Secretary to establish the reserve six months after submitting the plan to Congress. As of January 2017, DOE intended to submit its plan "in the near future."[89] In addition the DOE's efforts, six industry-led transformer-sharing programs are operating or being developed in the United States.[90]

There is widespread agreement among state and federal government officials, utilities, and manufacturers that HV transformers in the United States are vulnerable to terrorist attack, and that such an attack potentially could have catastrophic consequences. Congress has long been concerned about grid security in general, but recent security exercises, together with the Metcalf attack, have focused congressional interest on the physical security of HV transformers, among other specific aspects of the grid.[91] As the electric utility industry and federal agencies continue their efforts to improve the physical security of the grid, the 115th Congress may consider several key issues as part of its oversight of the sector: industry's implementation of the new physical security standards, DOE's plan for a strategic transformer reserve and related grid security activities, independent private sector efforts to improve HV transformer design and recovery, and the quality of federal information about threats to the grid.

(...continued)

No. 802, November 20, 2014.

[87] David Ortiz, Deputy Director, Office of Electric Reliability, Federal Energy Regulatory Commission, Remarks at the CRS seminar on *The Changing Electric Power Sector: Transmission and Grid Modernization*, December 9, 2016.

[88] U.S. Department of Energy, *Energy Transmission, Storage, and Distribution Infrastructure*, April 2015, p. 2-40.

[89] Government Accountability Office, *Electricity:Federal Efforts to Enhance Grid Resilience*, GAO-17-153, January 2017, p. 43.

[90] U.S. Department of Energy, *Transforming the Nation's Electricity System: The Second Installment of the QER*, January 2017, p. 4-48.

[91] See, for example: Senators Dianne Feinstein, Al Franken, Ron Wyden, and Harry Reid, letter to the Honorable Cheryl LaFleur, Acting Chairman, Federal Energy Regulatory Commission, February 7, 2014, http://www.ferc.gov/industries/electric/indus-act/reliability/chairman-letter-incoming.pdf.

Continuity of Government Operations

R. Eric Petersen, Specialist in American National Government, Government and Finance Division (epetersen@crs.loc.gov, 7-0643)

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

Current authority for executive branch continuity programs is provided in the 2007 National Security Presidential Directive (NSPD) on National Continuity Policy, NSPD-51.[92] To support the provision of essential government activities, NSPD-51 sets out a policy "to maintain a comprehensive and effective continuity capability composed of continuity of operations[93] and continuity of government[94] programs in order to ensure the preservation of our form of government[95] under the Constitution and the continuing performance of national essential functions (NEF) under all conditions."

Executive Order (E.O.) 12656, Assignment of Emergency Preparedness Responsibilities, was issued in 1988,[96] and assigns national security emergency preparedness responsibilities to federal executive departments and agencies. E.O. 12656 requires the head of each federal department and agency to "ensure the continuity of essential functions in any national security emergency by providing for: succession to office and emergency delegation of authority in accordance with applicable law; safekeeping of essential resources, facilities, and records; and establishment of emergency operating capabilities." Subsequent sections require each department to carry out specific contingency planning activities in its areas of policy responsibility.

Although contingency planning authorities are chiefly based on presidential directives, Congress could consider whether current authorities accurately reflect current government organization and goals, the costs of these programs, potential conflicts that might result from departments and

[92] White House, Office of the Press Secretary, *National Security and Homeland Security Presidential Directive*, May 9, 2007. NSPD-51 is also identified as Homeland Security Presidential Directive (HSPD) 20. A more detailed discussion of national continuity policy is available in CRS Report RS22674, *National Continuity Policy: A Brief Overview*, by R. Eric Petersen. Original document available at https://www.fema.gov/pdf/about/org/ncp/nspd_51.pdf.

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

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

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

[96] 53 *Federal Register* 47491; November 23, 1988.

agencies complying with different authorities, and the extent to which government contingency planning ensures that the federal executive branch will be able to carry out its responsibilities under challenging circumstances.

U.S. Secret Service

Shawn Reese, Analyst in Homeland Security Policy (sreese@crs.loc.gov, 7-0635)

For more information, see CRS Report R44197, *U.S. Secret Service: Selected Issues and Executive and Congressional Responses*.

Since 1865, the U.S. Secret Service (USSS) has investigated counterfeiting, and since 1901, at the request of congressional leadership, has provided full-time presidential protection.

Congress has increased its oversight of the USSS due to concern about terrorism threats, several security breaches, and misconduct of USSS personnel. A series of incidents has tarnished the image of the USSS and may have potentially affected its operations. For example, on September 19, 2014, a person gained unauthorized entrance into the White House after climbing the fence. On September 30, 2014, following a House Oversight and Government Reform Committee hearing on the USSS, which addressed this breach and previous incidents[97] it became public that on September 16, 2014, a private security contractor at a federal facility, while armed, was allowed to share an elevator with the President during a site visit, in violation of USSS security protocols. On March 4, 2015, it was reported that two senior USSS special agents, including one who was responsible for all aspects of White House security, disrupted the scene of an investigation of a suspicious package during an elevated security condition at the White House complex. It was further alleged that these two agents were under the influence of alcohol.

Both Congress and the USSS responded to the incidents. The USSS conducted a review of its training of personnel and its technology, perimeter security, and operations.[98] Congress conducted a number of oversight hearings on the incidents and USSS policy. At the end of the 114th Congress, one such hearing was conducted by the House Oversight and Government Reform Committee.[99] The purpose of this hearing was to examine allegations that USSS agents were not receiving compensation for overtime, and review DHS IG reports addressing USSS's protection of sensitive material. Among the criticisms raised at the hearing were assertions that

- the USSS' investigative mission places an additional burden on USSS agents and distracts from the Service's protection mission,
- the USSS suffers technology failures that cast doubts on the Service's ability to protect the nation's financial infrastructure,
- USSS agents are promoted to senior management positions despite alleged misconduct, and

[97] U.S. Congress, House Committee on Oversight and Government Reform, *White House Perimeter Breach: New Concerns about the Secret Service*, 113th Cong., 2nd sess., September 30, 2014.

[98] United States Secret Service Panel, *Report from the United States Secret Service Protective Mission Panel to the Secretary of Homeland Security*, Washington, DC, December 15, 2014. The executive summary is the only nonclassified portion of the report that is publicly available. The executive summary is available at http://www.dhs.gov/sites/default/files/publications/14_1218_usss_pmp.pdf.

[99] U.S. Congress, House Committee on Oversight and Government Reform, *Oversight of the Secret Service*, 114th Cong., 2nd sess., November 15, 2016.

- USSS senior leadership continues to withhold information pertaining to alleged misconduct from the committee.[100]

Congress is likely to continue to pursue these USSS issues in the 115th Congress.

Federal Facility Security

Shawn Reese, Analyst in Homeland Security Policy (sreese@crs.loc.gov, 7-0635)

For more information, see CRS Report R43570, *Federal Building and Facility Security: Frequently Asked Questions*.

The security of federal government buildings and facilities affects not only the daily operations of the federal government but also the health, well-being, and safety of federal employees and the public. Federal building and facility security is decentralized and disparate in approach, as numerous federal entities are involved, and some buildings or facilities are occupied by multiple federal agencies. The federal government is tasked with securing over 446,000 buildings and facilities daily.

The September 2001 terrorist attacks, the September 2013 Washington Navy Yard shootings, and the April 2014 Fort Hood shootings focused the federal government's attention on building security activities. This resulted in an increase in the security operations at federal facilities and more intense scrutiny of how the federal government secures and protects federal facilities, employees, and the visiting public.[101]

In general, federal facility security includes operations and policies that focus on reducing the exposure of the facility, employees, and the visiting public to criminal and terrorist threats. Each federal facility has unique attributes that reflect its individual security needs and the missions of the federal tenants. According to the Department of Justice's Office of Justice Programs (OJP), there are approximately 20 federal law enforcement entities that provide facility security.[102]

Due to the large number and different types of federal facilities, there is no single security standard that applies to every facility. There is, however, an interagency committee responsible for providing a number of standards that address federal facility security. The Interagency Security Committee's (ISC) mission is to "safeguard U.S. nonmilitary facilities from all hazards by developing state-of-the-art security standards in collaboration with public and private homeland security partners."[103]

Federal facility security is as diffuse as the number of law enforcement agencies securing them. Individual facilities secured by the same law enforcement agency may be secured in different manners based on specific security needs and threats. This makes it challenging to collect official and comprehensive data on threats to or incidents occurring at federal facilities.

[100] Ibid.

[101] See, for example, U.S. Congress, Senate Committee on Homeland Security and Governmental Affairs, *The Navy Yard Tragedy: Examining Physical Security for Federal Facilities*, 113th Cong., 1st sess., December 16, 2013, and U.S. Congress, House Committee on Transportation and Infrastructure, *Examining the Federal Protective Service: Are Federal Facilities Secure?*, 113th Cong., 2nd sess., May 21, 2014.

[102] U.S. Department of Justice, Bureau of Justice Statistics, http://www.bjs.gov/content/pub/pdf/fleo08.pdf.

[103] U.S. Department of Homeland Security, Interagency Security Committee, http://www.dhs.gov/about-interagency-security-committee.

DHS State and Local Preparedness Grants

Shawn Reese, Analyst in Homeland Security Policy (sreese@crs.loc.gov, 7-0635)

For more information, see CRS Report R44669, *Department of Homeland Security Preparedness Grants: A Summary and Issues*.

Congress has enacted legislation and appropriated grant funding to states and localities for homeland security purposes since 1996.[104] One of the first programs to provide this type of funding was the Nunn-Lugar-Domenici Program which was established by Congress in the 1996 Department of Defense Reauthorization Act[105] and provided assistance to over 150 cities for biological, chemical, and nuclear security. Providing homeland security assistance to states and localities was arguably spurred by the 1993 bombing of the World Trade Center in New York City and the 1995 bombing of the Alfred P. Murrah federal building in Oklahoma City. Following the September 11, 2001, terrorist attacks, Congress increased focus on state and local homeland security assistance by, among other things, establishing the Department of Homeland Security (DHS) and authorizing DHS to administer federal homeland security grant programs.[106]

With the increase of international and domestic terrorist threats and attacks against the United States following the end of the Cold War, and the termination of the old federal civil defense programs, a number of policy questions arose regarding homeland security assistance programs. The majority of these questions have not been completely addressed, even though Congress has debated and enacted legislation that provides homeland security assistance to states and localities since 1996.

Congressional debate continues on policy questions related to homeland security assistance for states and localities. Some may contend there is a need for the Congress to conduct further oversight hearings and legislate on policy issues related to DHS assistance to states and localities. These potential issues include (1) the purpose and number of assistance programs; (2) the use of grant funding; and (3) the funding level for the grant programs.

Generally, each grant program has a range of eligible activities. When Congress authorizes a federal grant program, the eligible activities may be broad or specific depending on the statutory language in the grant authorization. When grant funds are distributed through a competitive process, the administering federal agency officials exercise discretion in the selection of grant projects to be awarded funding within the range of eligible activities set forth by Congress.[107]

Some may argue the purpose and number of DHS grant programs have not been sufficiently addressed. Specifically, should DHS provide more all-hazards assistance versus terrorism-focused assistance? Does the number of individual grant programs result in coordination challenges and deficient preparedness at the state and local level? Would program consolidation improve domestic security? Finally, does the purpose and number of assistance programs affect the administration of the grants?

---

[104] For the purpose of this report, homeland security assistance programs are defined as Department of Homeland Security (DHS) programs, or programs that were transferred to DHS, which provide funding to states, localities, tribes, and other entities for security purposes; however, public safety and National Guard programs and funding are not included in this report. Additionally, the term "homeland security program" was not used until 2002. Prior to this, the term "domestic preparedness" was used to describe programs and activities that assisted states and localities to prepare for possible terrorist attacks.

[105] P.L. 104-106.

[106] P.L. 107-296.

[107] CRS Report R42769, *Federal Grants-in-Aid Administration: A Primer*, by Natalie Keegan.

Another issue Congress may address is how effectively DHS's assistance to states and localities is being spent. One way to review the use of program funding is to evaluate state and local jurisdictions' use of DHS's assistance. When DHS announces annual state and locality homeland security grant allocations, grant recipients submit implementation plans that identify how these allocations are to be obligated. However, the question remains whether or not the grant funding has been used in an effective way to enhance the nation's homeland security.

Annual federal support, through the appropriations process, for these homeland security grant programs is another issue Congress may want to examine considering the limited financial resources available to the federal government. Specifically, is there a need for the continuation of federal support for these programs, or should Congress reduce or eliminate funding? In the past 13 years, Congress has appropriated approximately $33 billion for state and local homeland security assistance. Since the establishment of DHS in 2003, Congress appropriated a high total of funding of $3.5 billion in FY2004, and the lowest appropriated amount was $1.4 billion in FY2013.

Border Security and Trade

Southwest Border Issues

Drug Trafficking and the Southwest Border

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

The United States is the world's largest marketplace for illegal drugs and sustains a multi-billion dollar market in illegal drugs.[108] An estimated 27.1 million Americans (10.1% of the 12 and older population) were current users of illicit drugs in 2015.[109] The most recent National Drug Threat Assessment Summary indicates that Mexican drug trafficking organizations continue to dominate the U.S. drug market.[110] The Drug Enforcement Administration (DEA) outlined this threat:

> Mexican [transnational criminal organizations (TCOs)] remain the greatest criminal drug threat to the United States; no other groups are currently positioned to challenge them.... By controlling lucrative smuggling corridors across the [Southwest border], Mexican TCOs are able to introduce multi-ton quantities of illicit drugs into the United States on a yearly basis. The poly-drug portfolio maintained by these Mexican TCOs consists primarily of heroin, methamphetamine, cocaine, marijuana, and, to a lesser extent, fentanyl.[111]

Mexican criminal networks either (1) transport or (2) produce and transport drugs north across the United States-Mexico border. After being smuggled across the border by criminal networks, the drugs are distributed and sold within the United States. The illicit proceeds may then be laundered or smuggled south across the border. While drugs are the primary goods trafficked by the criminal networks, those networks also generate income from other illegal activities, such as the

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

[109] Current means within the past month. U.S. Department of Health and Human Services, Substance Abuse and Mental Health Services Administration, *Key Substance Use and Mental Health Indicators in the United States: Results from the 2015 National Survey on Drug Use and Health*, September 2016.

[110] Drug Enforcement Administration, *2016 National Drug Threat Assessment Summary*, November 2016.

[111] Ibid., p. 1.

smuggling of humans and weapons, counterfeiting and piracy, kidnapping for ransom, and extortion.

One of the current domestic drug threats fueled, in part, by Mexican traffickers is heroin.[112] Not only has there been an increase in heroin use in the United States over the past several years, but there has been a simultaneous increase in its availability. This availability is driven by a number of factors, including increased production and trafficking of heroin by Mexican criminal networks.[113] Some Mexican farmers have reported abandoning marijuana cultivation in favor of growing opium poppies; the switch may be partly due to the decline in wholesale prices of marijuana in Mexico—which some claim is linked to increased marijuana legalization in the United States—and an increase in U.S. heroin demand.[114] Increases in Mexican heroin production and its availability in the United States have been coupled with increased heroin seizures at the Southwest border. Reportedly, these seizures increased by over 350% between 2008 and 2015.[115]

The 115th 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 the Obama Administration's National Southwest Border Counternarcotics Strategy, the overarching strategic goal of which was to "[s]ubstantially reduce the flow of illicit drugs, drug proceeds, and associated instruments of violence across the Southwest border."[116] Policymakers may also be interested in examining various federal drug control agencies' roles in reducing Southwest border trafficking. This could involve oversight of the DEA and its initiatives such as the Organized Crime Drug Enforcement Task Force (OCDETF) program, as well as the Office of National Drug Control Policy and its National Drug Control Strategy and Budget, among others.

Illicit Proceeds and the Southwest Border

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

The flow of money outside legal channels not only presents challenges to law enforcement, but it also has a significant nexus with homeland security policy. Proceeds from illegal enterprises are sometimes used to fund broader destabilizing activities, such as smuggling, illegal border crossings, or more violent activities, such as terrorist operations—including those controlled by the FARC (Revolutionary Armed Forces of Colombia) in Colombia.[117] While this is an issue with a global scope, this section focuses specifically on the policies affected by movement of illicit funds across the Southwest border.

As noted in the DEA's *National Drug Threat Assessment Summary*, "the annual volume of illicit proceeds generated in the United States is approximately $300 billion" and of that amount, "drug sales generate an estimated 21 percent, or $64 billion."[118] Money from the traffickers' illegal sale

[112] For more information on heroin trafficking in the United States, see CRS Report R44599, *Heroin Trafficking in the United States*, by Kristin Finklea.

[113] Drug Enforcement Administration, *2016 National Drug Threat Assessment Summary*, November 2016, p. 42.

[114] See, for example, Nick Miroff, "Tracing the U.S. Heroin Surge Back South of the Border as Mexican Cannabis Output Falls," *The Washington Post*, April 6, 2014.

[115] Drug Enforcement Administration, *2016 National Drug Threat Assessment Summary*, November 2016, p. 45.

[116] Office of National Drug Control Strategy, *National Southwest Border Counternarcotics Strategy*, 2013, p. 4.

[117] U.S. Department of State, *2016 International Narcotics Control Strategy Report: Volume II, Money Laundering and Financial Crimes*, March 2016.

[118] Drug Enforcement Administration, *2016 National Drug Threat Assessment Summary*, November 2016, p. 135.

of drugs in the United States is moved across the border into Mexico, and these funds fuel the drug traffickers' criminal activities. This money is often not deposited directly into the U.S. financial system; instead, it is illegally laundered through mechanisms such as bulk cash smuggling of U.S. currency into Mexico and "repatriation of the funds into the United States via couriers or armored vehicles."[119] Additionally, money may be moved through trade-based money laundering or placed in financial institutions, cash-intensive front businesses, prepaid or stored value cards, or money services businesses.[120]

The 115th Congress may examine interagency coordination to reduce the flow of illicit money (and other goods) across the Southwest border. Various departments and agencies—including the DEA, Federal Bureau of Investigation, U.S. Immigration and Customs Enforcement, U.S. Customs and Border Protection, and the Financial Crimes Enforcement Network (FinCEN)—share responsibility for combating drug-related activity and the flow of illicit proceeds both along the Southwest border and throughout the United States. Many of these agencies are also represented in Mexico, increasing U.S.-Mexican bilateral cooperation. Further, while some efforts explicitly target money laundering and bulk cash smuggling, other investigations might also uncover evidence of illicit proceeds. For instance, operations targeting southbound firearms smuggling may intercept individuals smuggling not only weapons, but cash proceeds from illicit drug sales as well.

Cross-Border Smuggling Tunnels

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

Mexican traffickers rely on cross-border tunnels to smuggle illicit drugs—primarily marijuana—from Mexico into the United States. At least 224 tunnels have been discovered along the Southwest border since the 1990s,[121] and some of the more recently discovered tunnels are highly sophisticated. Early tunnels were rudimentary "gopher hole" tunnels dug on the Mexican side of the border, traveling just below the surface, and popping out on the U.S. side as close as 100 feet from the border. Slightly more advanced tunnels relied on existing infrastructure, which may be shared by neighboring border cities such as Nogales, AZ, in the United States and Nogales, Sonora, in Mexico. These interconnecting tunnels may tap into storm drains or sewage systems, allowing smugglers to move drugs further and more easily than in tunnels they dug themselves. The most sophisticated tunnels can have rail, ventilation, and electrical systems. In April 2016 authorities uncovered the longest drug smuggling tunnel yet. At over 800 yards, it was equipped with railing, lighting, ventilation, and an elevator. Authorities seized over two thousand pounds of cocaine and over eleven tons of marijuana.[122]

U.S. law enforcement uses various tactics to detect these cross-border tunnels. They may use sonic equipment to detect the sounds of digging and tunnel construction and seismic technology to detect blasts that may be linked to tunnel excavation. Another tool for tunnel detection is

[119] U.S. Department of State, *2016 International Narcotics Control Strategy Report: Volume II, Money Laundering and Financial Crimes*, March 2016, p. 173.

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

[121] Drug Enforcement Administration, *2016 National Drug Threat Assessment Summary*, November 2016, p. 27.

[122] Department of Justice, U.S. Attorney's Office, Southern District of California, "Feds Seize Longest Tunnel on California-Mexico Border," press release, April 20, 2016.

ground penetrating radar.[123] However, factors including soil conditions, tunnel diameter, and tunnel depth can limit the effectiveness of this technology.

Despite these tools, U.S. officials have acknowledged that law enforcement currently does not have technology that is reliably able to detect sophisticated tunnels, and authorities have reportedly never found a tunnel with these technologies.[124] Rather, tunnels are more effectively discovered as a result of human intelligence and tips. U.S. officials have noted the value of U.S.-Mexican law enforcement cooperation in detecting, investigating, and prosecuting the criminals who create and use the cross-border tunnels.[125] As a result, the 115th Congress may not only consider how to best help U.S. law enforcement develop technologies that can keep pace with tunneling organizations, but also examine whether existing bi-national law enforcement partnerships are effective and whether they may be improved to enhance investigations of transnational criminals. Policymakers may also question how prominently the issue of combating cross-border smuggling tunnels may play within the larger border security framework.

Cargo Security

Lisa Sacco, Analyst in Illicit Drugs and Crime Policy (lsacco@crs.loc.gov, 7-7359)

For more information, see CRS Report R43014, *U.S. Customs and Border Protection: Trade Facilitation, Enforcement, and Security*, and CRS Report R43014, *U.S. Customs and Border Protection: Trade Facilitation, Enforcement, and Security*.

U.S. Customs and Border Protection (CBP), within DHS, is America's primary trade enforcement agency, and CBP seeks to balance the benefits of efficient trade flows against the demand for cargo security and the enforcement of U.S. trade laws. Thus, the overarching policy question with respect to incoming cargo is how to minimize the risk that weapons of mass destruction, illegal drugs, and other contraband will enter through a U.S. port of entry (POE), while limiting the costs and delays associated with such enforcement.

CBP's current trade strategy emphasizes "risk management" and a "multi-layered" approach to enforcement.[126] With respect to cargo security, risk management means that CBP segments importers into higher and lower risk pools and focuses security procedures on higher-risk flows, while expediting lower-risk flows. CBP's "multi-layered approach" means that enforcement occurs at multiple points in the import process, beginning before goods are loaded in foreign ports and continuing after the goods have been admitted into the United States. In recent years, congressional attention to cargo security has focused on one of CBP's primary tools for risk management, the Customs-Trade Partnership Against Terrorism (C-TPAT) trusted trader program, and on the statutory requirement that 100% of incoming maritime cargo containers be scanned

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

[124] Ron Nixon, "As Donald Trump Calls for Wall on Mexican Border, Smugglers Dig Tunnels," *The New York Times*, September 1, 2016. See also the statement of Laura E. Duffy, U.S. Attorney, Southern District of California, U.S. Department of Justice, before the U.S. Congress, Senate United States Senate Caucus on International Narcotics Control, *Illegal Tunnels on the Southwest Border*, 112th Cong., 1st sess., June 15, 2011.

[125] Ibid.

[126] See U.S. Customs and Border Patrol, *Vision and Strategy, 2020: U.S. Customs and Border Protection Strategic Plan*; and U.S. Congress, Senate Committee on Appropriations, Subcommittee on Department of Homeland Security, *Strengthening Trade Enforcement to Protect American Enterprise and Grow American Jobs*, 113th Cong., 2nd sess., July 16, 2014, Testimony of CBP Office of International Trade Acting Assistant Commissioner Richard DiNucci. The written testimony is available at https://www.dhs.gov/news/2014/07/16/written-testimony-cbp-senate-committee-appropriations-subcommittee-homeland-security.

abroad prior to being loaded on U.S.-bound ships. Congress also faces perennial questions about spending levels for POE infrastructure and personnel.

Customs-Trade Partnership Against Terrorism (C-TPAT)

Lisa Sacco, Analyst in Illicit Drugs and Crime Policy (lsacco@crs.loc.gov, 7-7359)

The Customs-Trade Partnership Against Terrorism (C-TPAT) is a voluntary public-private and international partnership that permits certain import-related businesses to register with CBP and perform security tasks prescribed by the agency. In return C-TPAT members are recognized as low-risk actors and are eligible for expedited import processing and other benefits.[127] CBP established C-TPAT in November 2001 following the September 11, 2001 (9/11) terrorist attacks, and the program was authorized as part of the Security and Accountability for Every Port Act of 2006 (SAFE Port Act, P.L. 109-347).

Proponents of C-TPAT favor increased participation in the program as a way to facilitate legal trade flows.[128] Some businesses, however, have criticized the program for providing inadequate membership benefits, especially in light of the time and financial investments required to become certified as C-TPAT members.[129]

Yet there may be no easy way to substantially expand C-TPAT benefits. In the case of land ports, the primary trusted trader benefit is access to dedicated lanes where wait times may be shorter and more predictable. However, adding lanes at land ports is difficult because many of them are located in urban areas with limited space for expansion and with limited ingress and egress infrastructure.[130] In the case of maritime imports, the primary trusted trader benefit is a reduced likelihood of secondary inspection.[131] Only about 6% of all maritime containers are selected for such an inspection,[132] so C-TPAT membership may offer little practical advantage in this regard.

In February 2017, the Government Accountability Office (GAO) issued a report outlining challenges in CBP management of the C-TPAT program. GAO recommended that CBP develop: "(1) standardized guidance for field offices regarding the tracking of information on security

[127] See U.S. CBP, "C-TPAT: Customs-Trade Partnership Against Terrorism," http://www.cbp.gov/border-security/ports-entry/cargo-security/c-tpat-customs-trade-partnership-against-terrorism. Commercial truck drivers who are Customs-Trade Partnership Against Terrorism (C-TPAT) members also are eligible to join the Free and Secure Trade System (FAST), which permits expedited processing at land ports of entry; and C-TPAT members who are residents of the United States and are known importers that have businesses physically established, located, and managed within the United States may be eligible for the Importer Self-Assessment Program (ISA), which exempts importers from certain post-entry enforcement audits. See ibid., and CBP FAST: Free and Secure Trade for Commercial Vehicles, http://www.cbp.gov/travel/trusted-traveler-programs/fast.

[128] See for example, U.S. Congress, Senate Committee on Homeland Security and Governmental Affairs, Evaluating Port Security: Progress Made and Challenges Ahead, 113th Cong., 2nd sess. June 4, 2014.

[129] See for example, U.S. Congress, House Committee on Ways and Means, Subcommittee on Trade, Supporting Economic Growth and Job Creation through Customs Trade Modernization, Facilitation, and Enforcement, 112th Cong., 2nd sess. May 17, 2012.

[130] See U.S. Department of Commerce, Draft Report: Improving Economic Outcomes by Reducing Border Delays, Facilitating the Vital Flow of Commercial Traffic Across the US-Mexican Border, Washington, DC, 2008, http://grijalva.house.gov/uploads/Draft%20Commerce%20Department%20Report%20on%20Reducing%20Border%20Delays%20Findings%20and%20Options%20March%202008.pdf

[131] Secondary inspection may include both nonintrusive imaging (NII) scans and/or physical inspection, in which the container may be opened and unpacked so that materials can be examined.

[132] Based on data provided to CRS by CBP on April 28, 2014.

validations, and (2) a plan with milestones and completion dates to fix the Dashboard so the C-TPAT program can produce accurate data on C-TPAT member benefits."[133]

100% Scanning Requirement

John Frittelli, Specialist in Transportation Policy (jfrittelli@crs.loc.gov, 7-7033), and Lisa Sacco, Analyst in Illicit Drugs and Crime Policy (lsacco@crs.loc.gov, 7-7359)

Section 1701 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L. 110-53) requires that all imported marine containers be scanned by nonintrusive imaging equipment and radiation detection equipment at a foreign loading port by July 1, 2012, unless DHS can demonstrate it is not feasible, in which case the deadline can be extended by two years on a port-by-port basis.

DHS has sought a blanket extension for all ports, citing numerous challenges to implementing the 100% scanning requirement at overseas ports.[134] In a report to Congress on the program, CBP identified three main obstacles to implementing 100% scanning at all foreign ports.[135] First, 100% scanning requires significant host state and private sector cooperation, but some foreign governments and business groups do not support 100% scanning. Second, 100% scanning would be logistically difficult. Initial pilots were deployed in relatively low-volume ports with natural chokepoints, but many cargo containers pass through large volume ports with more varied port architectures. Third, 100% scanning would be costly. In February 2012, the Congressional Budget Office (CBO) estimated that 100% scanning at foreign ports would cost an average of $8 million per shipping lane to implement, or a total of about $16.8 billion for all 2,100 shipping lanes.[136] Port operators and foreign partners also absorb additional costs associated with fuel and utilities, staffing, and related expenses. In a letter requesting renewal of the two-year extension, then-DHS Secretary Jeh Johnson stated,

> I have personally reviewed our current port security and DHS's short term and long term ability to comply with 100% scanning requirement. Following this review, I must report, in all candor, that DHS's ability to fully comply with this unfunded mandate of 100% scanning, even in the long term, is highly improbable, hugely expensive, and in our judgment, not the best use of taxpayer resources to meet this country's port security and homeland security needs.[137]

---

[133] Dashboard is a data reporting tool. U.S. Government Accountability Office, *Supply Chain Security: Providing Guidance and Resolving Data Problems Could Improve Management of the Customs-Trade Partnership Against Terrorism Program*, GAO-17-84, February 2017, http://www.gao.gov/assets/690/682620.pdf.

[134] Testimony of Janet Napolitano, Secretary of DHS, before the Committee on Commerce, Science, and Transportation, U.S. Senate, hearing "Transportation Security Challenges Post 9-11," December 2, 2009.

[135] See CBP, *Report to Congress on Integrated Scanning System Pilots (Security and Accountability for Every Port Act of 2006, §231),)*, http://www.apl.com/security/documents/sfi_finalreport.pdf. Also see U.S. GAO, *Supply Chain Security: Container Security Programs Have Matured, but Uncertainty Persists over the Future of 100 Percent Scanning*, GAO-12-422T, February 7, 2012, http://www.gao.gov/assets/590/588253.pdf. Also see letter from Janet Napolitano, Secretary of Homeland Security, to Hon. Joseph I. Lieberman, Senator, May 2, 2012.

[136] Spoken response by Kevin McAleenan, Acting Assistant Commissioner, Office of Field Operations, U.S. CBP, U.S. Department of Homeland Security, before the Border and Maritime Security Subcommittee of the Homeland Security Committee, U.S. House, hearing "Balancing Maritime Security and Trade Facilitation: Protecting Our Ports, Increasing Commerce and Securing the Supply Chain—Part I," February 7, 2012. CBP reports that the U.S. government spent a total of about $120 million during the first three years of the Secure Freight Initiative; CBP, *Report to Congress on Integrated Scanning System Pilots*, p. 13.

[137] Letter from DHS Secretary Jeh Johnson to Senator Carper, Chairman of the Senate Committee on Homeland Security and Governmental Affairs, May 5, 2014.

In an October 2015 hearing, DHS officials reiterated their opposition to a 100% scanning strategy in favor of a risk-based and layered security strategy.[138] Major U.S. trading partners also oppose 100% scanning. The European Commission has determined that 100% scanning is the wrong approach, favoring a multilayered risk management approach to inspecting cargo.[139] CBP has tested the feasibility of scanning all U.S.-bound containers at several overseas ports[140] and identified numerous operational, technical, logistical, financial, and diplomatic obstacles,[141] including opposition from host government officials.[142] In a July 2016 hearing, DHS officials restated their opposition to pursuing a 100% scanning strategy.[143] One-hundred-percent scanning conflicts with DHS's general approach to risk management, which seeks to focus scarce inspection resources on the highest-risk containers. By scanning a smaller number of containers, DHS may be able to devote additional resources to each individual scan. This alternative approach is considered important because reviewing the scans is labor-intensive, and scanning fewer containers may allow DHS to subject individual scans to greater scrutiny, and to maintain a lower threshold for opening containers with questionable scanning images.

If illicit cargo is estimated to be limited to less than 1% of incoming containers, as CBP believes to be the case, an alternative enforcement strategy may be to focus on a smaller set of only the likeliest containers. This approach would emphasize risk-based scanning along with investment in CBP intelligence to improve targeting, and/or increase CBP personnel, which would allow ports to conduct a larger number of targeted special enforcement operations.

Transportation Worker Identification Credential (TWIC)

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

In January 2007, TSA and the Coast Guard issued a final rule implementing the Transportation Worker Identification Credential (TWIC) at U.S. ports.[144] Longshoremen, port truck drivers, railroad workers, merchant mariners, and other workers at a port must apply for a TWIC card to obtain unescorted access to secure areas of port facilities or vessels.[145] The card was authorized under the Maritime Transportation Security Act of 2002 (MTSA; §102 of P.L. 107-295). As of October 2015, the population of TWIC holders was approximately 2.1 million.[146] The card must be renewed every five years.

---

[138] House Committee on Transportation and Infrastructure, Subcommittee on Coast Guard and Maritime Transportation, Hearing, *The Prevention of and Response to the Arrival of a Dirty Bomb at a U.S. Port*, October 27, 2015. In particular, see the oral and written testimonies of officials from CBP and the Domestic Nuclear Detection Office.

[139] European Commission Staff Working Paper, Secure Trade and 100% Scanning of Containers, February 2010, http://ec.europa.eu/taxation_customs/resources/documents/common/whats_new/sec_2010_131_en.pdf.

[140] This test was conducted as per Section 231 of the SAFE Port Act (P.L. 109-347).

[141] CBP, *Report to Congress on Integrated Scanning System Pilots (Security and Accountability for Every Port Act of 2006, §231)*, http://www.apl.com/security/documents/sfi_finalreport.pdf.

[142] Ibid, Appendix A.

[143] House Committee on Transportation and Infrastructure, Subcommittee on Coast Guard and Maritime Transportation, Hearing, *An Examination of the Maritime Nuclear Smuggling Threat and Other Port Security and Smuggling Risks in the U.S.*, July 7, 2016.

[144] 72 *Federal Register*, 3492-3604, January 25, 2007. Codified at 49 C.F.R. §1572.

[145] A TWIC does not entitle a card holder to access a maritime facility—the facility owner has the authority and responsibility to determine if the person has a legitimate business purpose for entering its facility.

[146] DHS, Office of Inspector General, "TWIC Background Checks are Not as Reliable as They Could Be," OIG-16-128, September 1, 2016, p. 2.

TSA conducts a security threat assessment of each worker before issuing a card. The security threat assessment uses the same procedures and standards established by TSA for truck drivers carrying hazardous materials, including examination of the applicant's criminal history, immigration status, and possible links to terrorist activity to determine whether a worker poses a security threat. A worker pays a fee of about $130 that is intended to cover the cost of administering the cards. The card uses biometric technology for positive identification. Terminal operators were to deploy card readers at the gates to their facilities, so that a worker's fingerprint template would be scanned each time he or she enters the port area and matched to the data on the card.

Finding a card reader that worked reliably in a harsh marine environment has proven difficult. On August 23, 2016, the Coast Guard issued a final rule requiring that only the highest-risk maritime facilities install card readers, generally facilities handling dangerous cargoes in bulk or large passenger vessels (> 1,000 passengers). This limited the facilities required to have card readers to about 525 facilities (about 16% of the roughly 3,200 maritime facilities regulated under MTSA). Other facilities, including those handling containerized cargo, would continue to use the TWIC as a "flash pass," but the biometric data on the card would not be used to positively identify the worker. Potential problems with this approach were highlighted by the February 2016 announcement that federal investigators uncovered a "document mill" producing fraudulent TWIC cards in Los Angeles.[147] The final rule becomes effective on August 23, 2018. Currently, the Coast Guard performs spot checks with hand-held biometric readers while conducting port security inspections.

GAO and Inspector General audits have been highly critical of how the TWIC has been implemented. A 2013 GAO audit found that the results of a pilot test of card readers should not be relied upon for developing regulations on card reader requirements because they were incomplete, inaccurate, and unreliable.[148] This audit was discussed at a hearing by the House Subcommittee on Government Operations on May 9, 2013,[149] and by the House Subcommittee on Border and Maritime Security on June 18, 2013.[150] Another 2013 GAO audit examined TSA's Adjudication Center (which performs security threat assessments on TWIC applicants and other transportation workers), and recommended steps the agency could take to better measure the center's performance.[151] A 2011 GAO audit found internal control weaknesses in the enrollment, background checking, and use of the TWIC card at ports, which were said to undermine the effectiveness of the credential in screening out unqualified individuals from obtaining access to port facilities.[152] Similarly, a 2016 Inspector General audit found that TSA appears to be more concerned with customer service in administering the cards (e.g., issuing them in a timely

[147] IHS Fairlplay Daily News, "Fake TWIC Cards Prompt U.S. Port Security Concerns," February 10, 2016.

[148] U.S. Government Accountability Office, *Transportation Worker Identification Credential—Card Reader Pilot Results Are Unreliable; Security Benefits Need to Be Reassessed*, GAO-13-198, May 8, 2013.

[149] U.S. Congress, House Committee on Oversight and Government Reform, Subcommittee on Government Operations, *Federal Government Approaches to Issuing Biometric IDs*, 113th Cong., 1st sess., May 9, 2013.

[150] U.S. Congress, House Committee on Homeland Security, Subcommittee on Border and Maritime Security, *Threat, Risk and Vulnerability: the TWIC Program*, 113th Cong., 1st sess., June 18, 2013.

[151] U.S. Government Accountability Office, *Transportation Security: Action Needed to Strengthen TSA's Security Threat Assessment Process*, GAO-13-629, July 19, 2013.

[152] U.S. Government Accountability Office, *Transportation Worker Identification Credential—Internal Control Weaknesses Need to Be Corrected to Help Achieve Security Objectives*, May 2011, GAO-11-657.

manner) than a careful scrutiny of applicants.[153] For instance, it found that applicants believed to be providing fraudulent identification documents were nevertheless issued a TWIC.

The 114th Congress enacted the Essential Transportation Worker Identification Credential Assessment Act (P.L. 114-278) which requires TSA to improve its vetting process, including fraud detection, and requires DHS to commission an outside organization to conduct a comprehensive assessment of the benefits and costs of the TWIC card.

Immigration Inspections at Ports of Entry (POEs)[154]

> For more information, see CRS Report R43356, *Border Security: Immigration Inspections at Ports of Entry*.

At ports of entry (POEs), Customs and Border Protection's (CBP's) Office of Field Operations (OFO) is responsible for conducting immigration, customs, and agricultural inspections of travelers seeking admission to the United States. The vast majority of people entering through U.S. ports are U.S. citizens, U.S. legal permanent residents (LPRs),[155] and legitimate visitors. Thus, CBP officers' goals are complex in that they are tasked with identifying and intercepting dangerous or unwanted (high-risk) people or materials, while also facilitating access for legitimate (low-risk) travelers. The Drug Enforcement Administration has cited the security risks present at POEs, noting that while transnational criminal organizations use a variety of methods to bring drugs across the border, "the most common method ... involves transporting drugs in vehicles through U.S. ports of entry (POEs)."[156] Transnational criminal organizations also transport drugs using commercial trains and busses, which too transit through the POEs.[157]

Travelers seeking admission at POEs are required to present a travel document, typically a passport or its equivalent[158] and (for non-U.S. citizens) either a visa authorizing permanent or temporary admission to the United States or proof of eligibility for admission through the Visa Waiver Program (VWP).[159] Foreign nationals are subject to security-related and other background checks prior to being issued a visa or to receiving travel authorization for the VWP. CBP officers at U.S. POEs verify the authenticity of travelers' documents and that each document belongs to the person seeking admission (i.e., confirm the traveler's identity). Identity confirmation relies in part on biometric checks against the Department of Homeland Security's (DHS) Automated Biometric Identification System (IDENT) database (see "Entry-Exit System" section, below). Database interoperability allows CBP officers to check travelers' records against other biographic and biometric databases managed by the Departments of Justice, State, and Defense.

The concentration of inspection activity at the border—for travelers and imports—means that sufficient resources must be present in order to minimize congestion and ensure efficient

---

[153] DHS, Office of Inspector General, "TWIC Background Checks are Not as Reliable as They Could Be," OIG-16-128, September 1, 2016

[154] Prepared by Carla Argueta, Analyst in Immigration Policy.

[155] Legal permanent residents (LPRs) are foreign nationals authorized to live lawfully and permanently within the United States. See CRS Report RL32235, *U.S. Immigration Policy on Permanent Admissions*, by Ruth Ellen Wasem.

[156] Drug Enforcement Administration, *National Drug Threat Assessment Summary 2016*, DEA-DCT-DIR-001-17, November 2016.

[157] Ibid.

[158] For more information on other acceptable documents, please see U.S. Customs and Border Protection, "Western Hemisphere Travel Imitative," https://www.cbp.gov/travel/us-citizens/western-hemisphere-travel-initiative.

[159] For a fuller discussion of travel requirements, see CRS Report RL31381, *U.S. Immigration Policy on Temporary Admissions* and CRS Report RL32221, *Visa Waiver Program*.

operations. CBP faces pressure to provide for the rapid processing of individuals crossing the border and must balance this demand with its goal of interdicting threats. Moreover, investment in POEs arguably has not kept pace with rapid growth in international travel and trade, and there may be inadequate infrastructure to manage flows at some ports of entry (also see "Port of Entry (POE) Infrastructure and Personnel" section, below).[160]

In an effort to streamline admissions without compromising security, CBP has implemented several trusted traveler programs. Trusted traveler programs require applicants to clear criminal and national security background checks prior to enrollment, to participate in an in-person interview, and to submit fingerprints and other biometric data.[161] In return, trusted travelers are eligible for expedited processing at POEs. CBP currently operates three main trusted traveler programs:

- Global Entry, which allows expedited screening of passengers arriving at 45 U.S. airports and 14 preclearance airports;[162]
- NEXUS, which is a joint U.S.-Canadian program for land, sea, and air crossings between the United States and Canada, including through dedicated vehicle lanes at 18 land ports;[163] and
- the Secure Electronic Network for Travelers Rapid Inspection (SENTRI), which allows expedited screening at land POEs on the U.S.-Mexican border, including through dedicated vehicle lanes at 10 land ports.[164]

Port of Entry (POE) Infrastructure and Personnel[165]

In light of the substantial flow of cargo and travelers at ports of entry, one perennial issue for Congress is how to allocate resources to Office of Field Operations (OFO) for POE personnel and infrastructure. Some in Congress have argued that inadequate personnel levels and infrastructure have contributed to costly delays and unpredictable wait times at ports of entry, particularly at land ports on the U.S.-Mexico border.[166]

---

[160] For example, Representative Jackson Lee stated, "our ports of entry are aging and their infrastructure can no longer accommodate the volume of trucks, vehicles, and pedestrians that cross every day, resulting in increasing wait times." U.S. Congress, House Committee on Homeland Security, Subcommittee on Border and Maritime Security, *Port of Entry Infrastructure: How does the Federal Government Prioritize Investments?*, 113th Cong., 2nd sess., July 16, 2014.

[161] Individuals are ineligible to participate in a trusted traveler program if they are inadmissible to the United States; provide false or incomplete information on trusted traveler applications; have been convicted of a criminal offense, have outstanding warrants, or are subject to an investigation; or have been found in violation of customs, immigration, or agriculture laws. Trusted travel enrollees are re-checked against certain security databases every 24 hours, every time they enter the United States, and every time they renew their trusted traveler membership.

[162] U.S. airports include airports in U.S. territories. Preclearance airports have airports in other countries, where CBP officers are placed in order to inspect travelers prior to boarding U.S.- bound flights. U.S. Customs and Border Protection, "Airports with Global Entry Kiosks," https://www.cbp.gov/travel/trusted-traveler-programs/global-entry/locations; U.S. Customs and Border Protection, "Preclearance Locations," https://www.cbp.gov/border-security/ports-entry/operations/preclearance.

[163] U.S. Customs and Border Protection, "NEXUS Land Border Crossings," https://www.cbp.gov/travel/trusted-traveler-programs/nexus/land-border-crossings.

[164] U.S. Customs and Border Protection, *Report on Business Transformation Initiatives*, September 2016.

[165] Prepared by Carla Argueta, Analyst in Immigration Policy.

[166] See, for example, U.S. Congress, House Committee on Homeland Security, Subcommittee on Border and Maritime Security, *Using Technology to Facilitate Trade and Enhance Security at Our Ports of Entry*, 112th Cong., 2nd sess., May 1, 2012. On border wait times, also see GAO, *CBP Action Needed to Improve Wait Time Data and Measure Outcomes of Trade Facilitation Effort*, GAO-13-603, July 24, 2013.

CBP's front-line enforcement personnel at POEs include CBP officers and agriculture specialists. In general, since 2004, Congress has invested more heavily in enforcement personnel between POEs (i.e., U.S. Border Patrol agents) than in law enforcement personnel at POEs (i.e., CBP officers).[167] However, the Homeland Security Appropriations Act, 2014 (P.L. 113-76) appropriated $256 million to increase the number of CBP officers at POEs by no fewer than 2,000 by the end of FY2015. CBP has yet to fully fill these positions due to challenges with its ability to recruit, hire, and retain personnel. Some recruitment issues include competition for personnel with other law enforcement agencies, the remote and undesirable locations of some positions, and a long and rigorous hiring process.[168] However, CBP reports that it has taken some steps to improve its recruitment, hiring, and retention processes.[169]

Congress created pilot programs that allow CBP to accept donations from stakeholders and/or to enter into reimbursable services agreement with them as a way to address the issues surrounding the balance of trade and travel facilitation with security protections.[170] The Donations Acceptance Program (DAP) allows CBP and the U.S. General Services Administration (GSA) to accept donations from private and public sector entities in the form of real property, personal property, and nonpersonal services.[171] Donations may be used for activities associated with the construction, alteration, operations, or maintenance of new or existing POEs.[172] The Reimbursable Services Program (RSP) enables CBP and private or public sector entities to partner in order to fund improvements in border facilities and port services, including hiring additional CBP officers and underwriting overtime hours.[173] These programs provide CBP with alternative sources of funding outside of the traditional congressional appropriations process.

Entry-Exit System[174]

Section 110 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA, P.L. 104-208, Div. C) required the Secretary of the DHS (formerly the Attorney General), to develop an automated entry and exit control system that would collect records of arrivals and departures and allow DHS to use these data to identify nonimmigrants[175] who remain

[167] Staffing for enforcement between POEs almost doubled from FY2004 to FY2016 (increasing from 10,819 to 19,828), while staffing at POEs increased just 27% during this period (from 18,110 to 22,910). U.S. Customs and Border Protection Office of Congressional Affairs in January 2013 and U.S. Customs and Border Protection, *Snapshot: A Summary of CBP Facts and Figures*, February 2016.

[168] U.S. Congress, House Committee on Homeland Security, Subcommittee on Border and Maritime Security, *Keeping Pace with Trade, Travel, and Security: How Does CBP Prioritize and Improve Staffing and Infrastructure?*, testimony by Office of Administration Assistant Commissioner Eugene Schied, CBP Human Resources Management Assistant Commissioner Linda Jacksta, and CBP Office of Field Operations Deputy Assistant Commissioner John Wagner, 114th Cong., 2nd sess., April 19, 2016.

[169] Ibid.

[170] The programs were first created under Section 559 of the Consolidated Appropriations Act, 2014 (P.L. 113-76) and were later authorized through the Cross-Border Trade Enhancement Act of 2016 (P.L. 114-279).

[171] For more information see https://www.cbp.gov/border-security/ports-entry/resource-opt-strategy/public-private-partnerships/donation-acceptance-program/program-and-process.

[172] This includes land acquisition, design, and the deployment of equipment and technologies. U.S. Customs and Border Protection, *Section 559 Donation Acceptance Authority: Proposal Evaluation Procedures and Criteria Framework*, 2014.

[173] For more information see https://www.cbp.gov/border-security/ports-entry/resource-opt-strategy/public-private-partnerships/reimbursable-services-program/program-and-partners.

[174] Prepared by Carla Argueta, Analyst in Immigration Policy.

[175] Nonimmigrants are foreign nationals who have been admitted to the United States temporarily and for a specific purpose.

in the United States beyond the periods of their visas. Congress amended the system's requirements and deadlines on several occasions since then, including requiring the entry-exit system to contain biometric technology and to be fully interoperable with the Departments of Justice and State's databases. The entry-exit system, however, remains incompletely implemented.[176]

The completion of the exit component of the system has been a persistent subject of congressional concern. No exit data are collected from persons leaving through southern border land POEs; and data collection at other POEs is limited to biographic data, is not always collected from a machine-readable document, and relies on information sharing with Canada and with air and sea carriers. CBP reportedly believes that for the purpose of exit tracking, biographic information sharing is cost effective.[177] At the same time, CBP has also argued that strengthened *biographic* data collection is a necessary precursor to effective *biometric* data collection, and it views a biometric system as a desirable long-term goal for the entry-exit system.[178] Furthermore, CBP has implemented various pilot programs at select POEs designed to test new technologies to verify travelers' identities.[179]

Enforcement Between Ports of Entry (POEs)[180]

> For more information, see CRS Report R42138, *Border Security: Immigration Enforcement Between Ports of Entry*.

Between POEs, CBP's U.S. Border Patrol is responsible for enforcing U.S. immigration law and other federal laws along the border and for preventing all unlawful entries into the United States, including entries of terrorists, unauthorized migrants, instruments of terrorism, narcotics, and other contraband. The Border Patrol, in the course of discharging its duties, patrols 7,494 miles of U.S. international borders with Mexico and Canada and the coastal waters around Florida and Puerto Rico.

With support from Congress, CBP—and its predecessor agency the Immigration and Naturalization Service (INS)—has invested in border security personnel, fencing and infrastructure, and surveillance technology since the 1980s, with CBP's current budget totaling $13.3 billion in FY2016.[181] However, some Members of Congress have raised questions about whether CBP's investments at the border have been effective.[182] More recently, the Trump

[176] For more information, see U.S. Department of Homeland Security, *Comprehensive Biometric Entry/Exit Plan*, April 2016.

[177] Testimony of DHS Assistant Secretary David Heyman, U.S. Congress, House Committee on Judiciary, *Implementation of an Entry-Exit System: Still Waiting After All These Years*, 113th Cong., 1st sess., November 13, 2013. Hereinafter: Heyman Testimony, 2013.

[178] See for example Testimony of CBP Deputy Assistant Commissioner John Wagner, U.S. Congress, House Committee on Oversight and Government Affairs, Subcommittee on National Security, *Border Security Oversight, Part III: Border Crossing Cards and B1/B2 Visas*, 113th Cong., 1st sess., November 14, 2013.

[179] For more information, see https://www.cbp.gov/travel/biometric-security-initiatives.

[180] Prepared by Carla Argueta, Analyst in Immigration Policy.

[181] For a fuller discussion of FY2016 appropriations, see CRS Report R44215, *DHS Appropriations FY2016: Security, Enforcement and Investigations*, coordinated by William L. Painter.

[182] See for example, U.S. Congress, House Committee on Homeland Security, Subcommittee on Border and Maritime Security, *A Study in Contrasts: House and Senate Approaches to Border Security*, 113th Cong., 1st sess., July 23, 2013. The Border Patrol published a national strategy for controlling U.S. borders in May 2012, building on three earlier strategies published between 1994 and 2005. The new strategy describes the Border Patrol's approach to risk management and to striking a balance among its traditional emphasis on preventing unauthorized migration and its (continued...)

Administration has shown interest in increasing resources on the Southwest border. For instance, President Trump signed Executive Order 13767 on January 25, 2017, calling for the immediate planning, designing, and construction of a "physical wall" along the Southwest border[183] and the hiring of an additional 5,000 Border Patrol agents.[184]

Congress also has raised questions about how to measure border security. The CBP has used several different border security metrics that focused on border enforcement outputs, such as the number of migrants apprehended, the migrant interdiction rate, and the recidivism rate (previously removed migrants that re-attempt to cross the border without authorization). These metrics all have limitations. For instance, it is difficult to separate the effects of border security efforts from other factors, such as the economic, political, and social realities present in migrants' home countries and the United States. Most recently, CBP has used statistical modeling to estimate a new border security metric, the level of successful unauthorized entry of migrants into the United States. This metrics seeks to describe the flow of migrants into the United States but may not directly speak to border security effectiveness.[185]

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

Aviation Security

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

For more information, see CRS Report RL33512, *Transportation Security: Issues for the 115th Congress*, by Bart Elias, David Randall Peterman, and John Frittelli

Following the 9/11 terrorist attacks, Congress took swift action to create the Transportation Security Administration (TSA), federalizing all airline passenger and baggage screening functions and deploying significantly increased numbers of armed air marshals on commercial passenger flights. Despite the extensive focus on aviation security for more than a decade, a number of challenges remain, including

- effectively screening passengers, baggage, and cargo for explosives threats;

(...continued)

post-9/11 priority missions of preventing the entry of terrorists and terrorist weapons, along with the recent U.S. focus on combating transnational criminal organizations. The strategy does not describe operational plans or address the interaction among the Border Patrol and other federal agencies (including other parts of DHS) with responsibilities at the border.

[183] There are currently approximately 654 miles of border fencing along the southwest border with Mexico. U.S. Government Accountability Office, *Southwest Border Security: Additional Actions Needed to Better Assess Fencing's Contributions to Operations and Provide Guidance for Identifying Capability Gaps*, GAO-17-331, February 2017.

[184] Executive Order 13767, "Border Security and Immigration Enforcement Improvements," 82 *Federal Register* 8793-8797, January 25, 2017.

[185] For more information, see CRS Report R44386, *Border Security Metrics Between Ports of Entry* and John W. Bailey, Sarah K. Burns, and David F. Eisler, *Assessing Southwest Border Security*, Institute for Defense Analysis, May 2016.

[186] See, e.g., U.S. Government Accountability Office, *Border Security: Enhanced DHS Oversight and Assessment of Interagency Coordination is Needed for the Northern Border*, GAO-11-97, December 2010. Also see CRS Report R42969, *Border Security: Understanding Threats at U.S. Borders*, by Jerome P. Bjelopera and Kristin Finklea.

- developing effective risk-based methods for screening passengers and others with access to aircraft and sensitive areas;
- exploiting available intelligence information and watchlists to identify individuals who pose potential threats to civil aviation;
- effectively responding to security threats at airports and screening checkpoints;
- developing effective strategies for addressing aircraft vulnerabilities to shoulder-fired missiles and similar weapons; and
- addressing the potential security implications of unmanned aircraft operations in domestic airspace.

Explosives Screening Strategy for the Aviation Domain

The Aviation and Transportation Security Act (ATSA; P.L. 107-71) mandated 100% screening of all checked baggage placed on domestic passenger flights and on international passenger flights to and from the United States. In addition, the Implementing the 9/11 Commission Recommendations Act of 2007 (P.L. 110-53) mandated the physical screening of all cargo placed on passenger flights. Unlike passenger and checked baggage screening, TSA does not routinely perform physical inspections of air cargo. Rather, TSA satisfies this mandate through the Certified Cargo Screening Program. Under the program, manufacturers, warehouses, distributors, freight forwarders, and shippers carry out screening inspections using TSA-approved technologies and procedures both at airports and at off-airport facilities in concert with certified supply-chain security measures and chain of custody standards.

Internationally, TSA works with other governments, international trade organizations, and industry to assure that all U.S.-bound and domestic cargo carried aboard passenger aircraft meets the requirements of the mandate. Additionally, TSA works closely with Customs and Border Protection (CBP) to carry out risk-based targeting of cargo shipments, including use of the CBP Advance Targeting System-Cargo (ATS-C), which assigns risk-based scores to inbound air cargo shipments to identify shipments of elevated risk. Originally designed to combat drug smuggling, ATS-C has evolved over the years, particularly in response to the October 2010 cargo aircraft bomb plot that originated in Yemen, to assess shipments for explosives threats or other terrorism-related activities.

In response to a 2009 incident aboard a Northwest Airlines flight, the Obama Administration accelerated deployment of Advanced Imaging Technology (AIT) whole body imaging screening devices and other technologies at passenger screening checkpoints. This deployment also responded to the 9/11 Commission recommendation to improve the detection of explosives on passengers.[187] Explosives screening technologies at passenger screening checkpoints primarily consist of whole body imaging systems known as Advanced Imaging Technology (AIT); advanced technology X-ray imagers for carry-on items; and explosives trace detection (ETD) systems used to test swab samples collected from individuals or carry-on items for explosives residue. In its FY2017 budget request, TSA indicated that it intends to procure AIT and ETD systems in small numbers, while it intends to acquire more than 300 advanced technology X-ray imagers for carry-on items, upgraded with multi-view capabilities or automated explosives detection capabilities.

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

The use of AIT has raised a number of policy questions. Privacy advocates have objected to the intrusiveness of AIT, particularly when used for primary screening.[188] To allay privacy concerns, TSA eliminated the use of human analysis of AIT images and does not store imagery. In place of human image analysts, TSA has deployed automated targeting recognition (ATR) software that generates generic avatar images indicating locations of possible threat items. Another concern raised about AIT centered on the potential medical risks posed by backscatter X-ray systems, but those systems are no longer in use for airport screening, and current millimeter wave systems emit nonionizing millimeter waves are not considered harmful.

The effectiveness of AIT and ATR has been brought into question. In 2015, the DHS Office of Inspector General completed covert testing of passenger screening checkpoint technologies and processes to evaluate the effectiveness of AIT and ATR.[189] In congressional testimony, DHS Inspector General John Roth revealed that the covert testing consistently found failures in technology and procedures coupled with human error that allowed prohibited items to pass into secure areas.[190] Even prior to the revelations of weaknesses in passenger checkpoint screening technologies and procedures, the use of AIT was controversial. Past legislative proposals specifically sought to prohibit the use of whole body imaging for primary screening (see, for example, H.R. 2200, 111th Congress). Nonetheless, primary screening using AIT is now commonplace at larger airports. Checkpoints at many smaller airports have not been furnished with AIT equipment or other advanced checkpoint detection technologies.

In addition to continued deployment and utilization of AIT, the FAA Extension, Safety, and Security Act of 2016 (P.L. 114-190) directed TSA to task the Aviation Security Advisory Committee, composed of industry experts on airport and airline security matters, to develop recommendations for more efficient and effective passenger screening. It also directed TSA to initiate a pilot program at three to six large airports to examine passenger checkpoint reconfigurations that increase efficiencies and reduce vulnerabilities, and a separate pilot program at three airports to develop and test next-generation screening system prototypes designed to expedite passenger handling.

For checked baggage screening, TSA utilizes explosives detection system (EDS) and ETD technology. TSA deploys either high-speed (greater than 900 bags per hour), medium-speed (400 to 900 bags per hour), or reduced-size (100 to 400 bags per hour) EDS systems, depending on airport needs and configurations. The use of explosives detection technology was mandated by the Aviation and Transportation Security Act (ATSA; P.L. 107-71) more than a decade ago. Consequently, present TSA checked-baggage explosives detection technology acquisition is primarily focused on replacing systems that have reached the end of their service lives. TSA is also funding the development of new algorithms to more reliably detect homemade explosives threats in checked baggage and reduce false positives. TSA pays for or reimburses airports for modifying baggage-handling facilities and installing new inspection systems to accommodate explosives detection technologies.

The TSA's National Explosives Detection Canine Team Program trains and deploys canines and handlers at transportation facilities to detect explosives. The program includes approximately 320

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

[189] Department of Homeland Security, Office of Inspector General, *DHS OIG Highlights: Covert Testing of the Transportation Security Administration's Passenger Screening Technologies and Processes at Airport Security Checkpoints*, OIG-15-150, September 22, 2015.

[190] Statement of John Roth, Inspector General, Department of Homeland Security, Before the Committee on Oversight and Government Reform, U.S. House of Representatives, Concerning TSA: Security Gaps, November 3, 2015.

TSA teams and 675 state and local law enforcement teams trained by TSA under partnership agreements. More than 180 of the TSA teams are dedicated to passenger screening at about 40 airports. Following airport bombings in Brussels, Belgium, and Istanbul, Turkey, in 2016, there has been interest in increasing deployments of canine teams in nonsterile areas of airport terminals.

P.L. 114-190 included language authorizing TSA to provide training to foreign governments in airport security measures including the use of canine teams. The act also directed TSA to utilize canine teams along with other resources and technologies to minimize passenger wait times and maximize security effectiveness of checkpoint operations.

Risk-Based Passenger Screening

TSA has initiated a number of initiatives to focus its resources based on intelligence-driven assessments of security risk. These include the PreCheck trusted traveler program; modified screening procedures for children 12 and under; and a program for expedited screening of known flight crew and cabin crew members. Programs have also been developed for modified screening of elderly passengers similar to those procedures put in place for children.

PreCheck is TSA's latest version of a trusted traveler program that has been modeled after CBP programs such as Global Entry, SENTRI, and NEXUS. Under the PreCheck program, participants vetted through a background check process are processed through expedited screening lanes where they can keep shoes on and keep liquids and laptops inside carry-on bags. As of December 2016, PreCheck expedited screening lanes were available at more than 180 airports. The cost of background checks under the PreCheck program is recovered through application fees of $85 per passenger for a five-year membership. TSA's goal is to process 50% of passengers through PreCheck expedited screening lanes, thus reducing the need for standard security screening lanes, but it has struggled to increase program membership. About 10 million individuals have enrolled in either PreCheck or other DHS trusted traveler programs, like Global Entry, that allow access to expedited screening lanes. TSA would like to boost this number to 25 million.[191]

P.L. 114-190 included language requiring TSA to increase the involvement of private-sector entities in marketing PreCheck and enrolling applicants. The law also mandates that PreCheck lanes be open and available during peak and high-volume travel times.

One concern raised over the PreCheck program, however, is the lack of biometric authentication to verify participants at screening checkpoints. A predecessor test program, the Registered Traveler program, which used private vendors to issue and scan participants' biometric credentials, was scrapped by TSA in 2009 because it failed to show a demonstrable security benefit. In 2016, biometric identity authentication was reintroduced at 13 airports under a private trusted traveler program known as Clear. Participants in Clear, which is separate from PreCheck and not operated or funded by TSA, use an express lane to verify identity using a fingerprint or iris scan rather than interacting with a TSA document checker.[192]

Questions remain regarding whether PreCheck is fully effective in directing security resources to unknown or elevated-risk travelers. Nonetheless, it has improved screening efficiency, resulting

[191] Kelly Yamanouchi, "Haven't Joined TSA PreCheck Yet? You're Not Alone," *Atlanta Journal Constitution*, June 17, 2016, http://airport.blog.ajc.com/2016/06/14/havent-joined-tsa-precheck-yet-youre-not-alone/.

[192] Scott McCartney, "The Airport Security Shortcut That Isn't PreCheck," *Wall Street Journal*, June 22, 2016, http://www.wsj.com/articles/the-airport-security-short-cut-that-isnt-precheck-1466616335.

in cost savings for TSA. TSA estimates annual savings in screener workforce costs totaling $110 million as a result of PreCheck and other risk-based initiatives.[193]

TSA has also developed a passenger behavior detection program to identify potential threats based on observed behavioral characteristics. TSA initiated early tests of its Screening Passengers by Observational Techniques (SPOT) program in 2003. By FY2012, the program deployed almost 3,000 behavioral detection officers at 176 airports, at an annual cost of about $200 million. Questions remain regarding the effectiveness of the behavioral detection program, and privacy advocates have cautioned that it could devolve into racial or ethnic profiling. While some Members of Congress have sought to shutter the program, Congress has not moved to do so. For example, H.Amdt. 127 (113th Congress), an amendment to the FY2014 DHS appropriations measure that sought to eliminate funding for the program, failed to pass a floor vote. Congress also has not taken specific action to revamp the program, despite the concerns raised by GAO and the DHS Office of Inspector General.[194]

The Use of Terrorist Watchlists in the Aviation Domain

Airlines were formerly responsible for checking passenger names against terrorist watchlists maintained by the government. Following at least two instances in 2009 and 2010 in which such checks failed to identify individuals who may pose a threat to aviation, TSA modified security directives to require airlines to check passenger names against the no-fly list within two hours of being electronically notified of an urgent update, instead of allowing 24 hours to recheck the list. The event also accelerated the transfer of watchlist checks from the airlines to TSA under the Secure Flight program. In November 2010, DHS announced that 100% of passengers flying to or from U.S. airports are being vetted using the Secure Flight system.[195]

Secure Flight vets passenger name records against a subset of the Terrorist Screening Database (TSDB). On international flights, Secure Flight operates in coordination with the use of watchlists by CBP's National Targeting Center-Passenger, which relies on the Advance Passenger Information System (APIS) and other tools to vet both inbound and outbound passenger manifests. In addition to these systems, TSA conducts risk-based analysis of passenger data carried out by the airlines through use of the Computer-Assisted Passenger Prescreening System (CAPPS). In January 2015, TSA gave notification that it would start incorporating the results of CAPPS assessments, but not the underlying data used to make such assessments, into Secure Flight, along with each passenger's full name, date of birth, and PreCheck traveler number (if applicable). These data are used within the Secure Flight system to perform risk-based analyses to determine whether passengers receive expedited, standard, or enhanced screening at airport checkpoints.[196]

---

[193] Department of Homeland Security, Transportation Security Administration, *Fiscal Year 2016 Congressional Justification, Aviation Security*, p. 5. All FY2016 DHS budget justifications are available at https://www.dhs.gov/publication/congressional-budget-justification-fy-2016 as a single file.

[194] U.S. Government Accountability Office, *Aviation Security: TSA Should Limit Future Funding for Behavior Detection Activities*, GAO-14-159, November 2013; Department of Homeland Security, Office of Inspector General, *Transportation Security Administration's Screening of Passengers by Observation Techniques (Redacted)*, OIG-13-91, Washington, DC, May 29, 2013; Department of Homeland Security, Statement of Charles K. Edwards, Deputy Inspector General, Before the United States House of Representatives, Committee on Homeland Security, Subcommittee on Transportation Security, November 13, 2013.

[195] Department of Homeland Security, "DHS Now Vetting 100 Percent of Passengers on Flights Within or Bound for U.S. Against Watchlists," Press Release, November 30, 2010.

[196] Department of Homeland Security, Transportation Security Administration, "Privacy Act of 1974; Department of (continued...)

Central issues surrounding the use of terrorist watchlists in the aviation domain that may be considered during the 115th Congress include the speed with which watchlists are updated as new intelligence information becomes available; the extent to which all information available to the federal government is exploited to assess possible threats among passengers and airline and airport workers; the ability to detect identity fraud or other attempts to circumvent terrorist watchlist checks; the adequacy of established protocols for providing redress to individuals improperly identified as potential threats; and the adequacy of coordination with international partners.[197] In addition, there has been a growing interest in finding better ways to utilize watchlists to prevent terrorist travel, particularly travel of radicalized individuals seeking to join forces with foreign terrorist organizations such as the Islamic State (IS).[198]

Language in P.L. 114-190 directed TSA to assess whether recurrent fingerprint-based criminal background checks could be carried out in a cost-effective manner to augment terrorist watchlist checks for PreCheck program participants. Additionally, the act directed TSA to expand criminal background checks for certain airport workers.

Perimeter Security, Access Controls, and Worker Vetting

Airport perimeter security, access controls, and credentialing of airport workers are generally responsibilities of airport operators. There is no common access credential for airport workers. Rather, each airport issues its own security credentials to airport workers. These credentials are often referred to as Security Identification Display Area (SIDA) badges, and they convey the level of access that an airport worker is granted.

TSA requires access control points to be secured by measures such as posted security guards or electronically controlled locks. Additionally, airports must implement programs to train airport employees to look for proper identification and challenge anyone not displaying proper identification.

Airports may also deploy surveillance technologies, access control measures, and security patrols to protect airport property from intrusion, including buildings and terminal areas. Such measures are paid for by the airport, but must be approved by TSA as part of an airport's overall security program. State and local law enforcement agencies with jurisdiction at the airport are generally responsible for patrols of airport property, including passenger terminals. They also may patrol adjacent properties to deter and detect other threats to aviation, such as shoulder-fired missiles (see "Mitigating the Threat of Shoulder-Fired Missiles to Civilian Aircraft").

TSA requires security background checks of airport workers with unescorted access privileges to secure areas at all commercial passenger airports and air cargo facilities. Background checks consist of a fingerprint-based criminal history records check and security threat assessment, which include checking employee names against terrorist database information. Certain criminal offenses committed within the past 10 years, including aviation-specific crimes, transportation-related crimes, and other felony offences, are disqualifying.

(...continued)

Homeland Security Transportation Security Administration-DHS/TSA-019 Secure Flight Records System of Records," 80 *Federal Register* 233-239, January 5, 2015.

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

[198] For further details see CRS Report R44678, *The Terrorist Screening Database and Preventing Terrorist Travel*, by Jerome P. Bjelopera, Bart Elias, and Alison Siskin, and CRS Report R43730, *Terrorist Databases and the No Fly List: Procedural Due Process and Other Legal Issues*, by Jared P. Cole.

P.L. 114-190 directed TSA to update the eligibility criteria and disqualifying criminal offenses for SIDA access credentials based on other transportation vetting requirements and knowledge of insider threats to security. The law proposes that TSA expand the criminal history look-back period from the current 10 years to 15 years, and that individuals be disqualified if they have been released from prison within five years of their application. The statute directs TSA to establish a formal waiver process for individuals denied credentials. It also calls for full implementation of recurrent vetting of airport workers with SIDA access credentials using the Federal Bureau of Investigation's Rap Back services to identify disqualifying criminal offences.

Language in P.L. 114-190 also directs TSA to conduct enhanced physical inspections of airport workers at SIDA access points and in SIDA areas. The inspections are to be random and unpredictable as well as data-driven and operationally dynamic. The law also directs TSA and the Department of Homeland Security Office of Inspector General to increase covert testing of access controls.

Security Incidents at Airports

Incident response at airports is primarily the responsibility of the airport operator and state or local law enforcement agencies, with TSA acting as a regulator in approving response plans as part of an airport's comprehensive security program.

On November 1, 2013, a lone gunman targeting TSA employees fired several shots at a screening checkpoint at Los Angeles International Airport (LAX), killing one TSA screener and injuring two other screeners and one airline passenger. In a detailed post-incident action report, TSA identified several proposed actions to improve checkpoint security, including enhanced active shooter incident training for screeners; better coordination and dissemination of information regarding incidents; expansion and routine testing of alert notification capabilities; and expanded law enforcement presence at checkpoints during peak times. TSA did not support proposals to arm certain TSA employees or provide screeners with bulletproof vests, and did not recommend mandatory law enforcement presence at checkpoints.

The Gerardo Hernandez Airport Security Act of 2015 (P.L. 114-50), named in honor of the TSA screener killed in the LAX incident and enacted in September 2015, requires airports to adopt plans for responding to security incidents. Additionally, the act requires TSA to create a mechanism for sharing information among airports regarding best practices for airport security incident planning, management, and training. It also requires TSA to identify ways to expand the availability of funding for checkpoint screening law enforcement support through cost savings from improved efficiencies. Law enforcement response to incidents at passenger screening checkpoints allows for flexibility in the deployment of law enforcement support. While some airports station law enforcement officers at dedicated posts at or near passenger screening checkpoints, other airports allow officers to patrol other areas of the airport so long as a minimum response time to incidents at passenger screening checkpoints is maintained. TSA provides funding for law enforcement support at screening checkpoints through agreements that partially reimburse for law enforcement hours.

The Brussels and Istanbul airport bombings in 2016 increased concern over response to security incidents in nonsterile areas of airports prior to passenger screening checkpoints. Language in P.L. 114-190 establishes requirements for DHS to develop training exercises to enhance law enforcement and first responder preparedness for active shooter and mass casualty events at airports, mass transit systems, and other public locations.

Foreign Last Point of Departure Airports

TSA regulates foreign air carriers that operate flights to the United States to enforce requirements regarding the acceptance and screening of passengers, baggage, and cargo carried on those aircraft.[199] As part of this regulation, TSA inspects foreign airports from which commercial flights proceed directly to the United States.

Fifteen foreign last point of departure airports (eight in Canada, two in the Bahamas, one in Bermuda, one in Aruba, two in Ireland, and one in Abu Dhabi) have Customs and Border Protection preclearance facilities where passengers are admitted to the United States prior to departure. Passengers on international flights from these preclearance airports deplane directly into the airport sterile area upon arrival at the U.S. airport of entry; they may then board connecting flights or leave the airport directly, rather than being routed to customs and immigration processing facilities. Assessing screening measures at preclearance airports is a particular priority for TSA. TSA is also working to increase checked baggage preclearance processing so checked baggage does not have to be rescreened by TSA at the airport of entry, which has been the practice.[200]

Language in P.L. 114-190 requires TSA to conduct security risk assessments at all last point of departure airports, and authorizes the donation of security screening equipment to such airports to mitigate security vulnerabilities that put U.S. citizens at risk.

Mitigating the Threat of Shoulder-Fired Missiles to Civilian Aircraft

The threat to civilian aircraft posed by shoulder-fired missiles or other standoff weapons capable of downing an airliner remains a vexing concern for aviation security specialists and policymakers. The terrorist threat posed by small man-portable shoulder-fired missiles was brought into the spotlight soon after the 9/11 terrorist attacks by the November 2002 attempted downing of a chartered Israeli airliner in Mombasa, Kenya, the first such event outside of a conflict zone. Since then, Department of State and military initiatives seeking bilateral cooperation and voluntary reductions of man-portable air defense systems (MANPADS) stockpiles had reduced worldwide inventories by nearly 33,000 missiles.[201] Despite this progress, such weapons may still be in the hands of terrorist organizations. Conflicts in Libya and Syria have renewed concerns that large military stockpiles of these weapons may be proliferated to radical insurgent groups like Ansar al-Sharia in Libya, Al Qaeda in the Islamic Maghreb (AQIM), and the Islamic State (IS).[202] The most visible DHS initiative to address the threat was the multiyear Counter-MANPADS program carried out by the DHS Science and Technology

[199] See 49 C.F.R. Part 1546.

[200] Department of Homeland Security, *Congressional Budget Justification, FY2017—Volume II: Transportation and Security Administration, Operations and Support*, p. 46.

[201] U.S. Department of State, *Addressing the Challenge of MANPADS Proliferation*, Remarks of Andrew J. Shapiro, Assistant Secretary, Bureau of Political-Military Affairs, Stimson Center, Washington, DC, February 2, 2012, https://www.state.gov/t/pm/rls/rm/183097.htm; Andrew J. Shapiro, Assistant Secretary, Bureau of Political-Military Affairs, U.S. Department of State, Addressing the Challenge of MANPADS Proliferation, Remarks, Stimson Center, Washington, DC, February 2, 2012, http://www.state.gov/t/pm/rls/rm/183097.htm.

[202] See Andrew J. Shapiro, Assistant Secretary, Bureau of Political-Military Affairs, U.S. Department of State, Addressing the Challenge of MANPADS Proliferation, Remarks, Stimson Center, Washington, DC, February 2, 2012, http://www.state.gov/t/pm/rls/rm/183097.htm; Thomas Gibbons-Neff, "Islamic State Might Have Taken Advanced MANPADS from Syrian Airfield," *Washington Post*, August 24, 2014; Sharyl Attkisson, "Thousands of Libyan Missiles from Qaddafi Era Missing in Action," CBS News, March 25, 2013, http://www.cbsnews.com/news/thousands-of-libyan-missiles-from-qaddafi-era-missing-in-action/.

Directorate. The program concluded in 2009 with extensive operational and live-fire testing along with Federal Aviation Administration (FAA) certification of two systems capable of protecting airliners against heat-seeking missiles. The systems have not been deployed on commercial airliners in the United States, however, due largely to high acquisition and life-cycle costs. MANPADS are mainly seen as a security threat to civil aviation overseas, but a MANPADS attack in the United States could have a considerable impact on the airline industry. While major U.S. airports have conducted vulnerability studies, efforts to reduce vulnerabilities of flight paths to potential MANPADS attacks face significant challenges because of limited resources and large geographic areas where aircraft are vulnerable to attack. Any terrorist attempts to exploit those vulnerabilities could quickly escalate the threat of shoulder-fired missiles to a major national security priority.

Security Issues Regarding the Operation of Unmanned Aircraft

The operation of civilian unmanned aerial systems (UASs) in domestic airspace raises potential security risks, including the possibility that terrorists could use a drone to carry out an attack against a ground target. It is also possible that drones themselves could be targeted by terrorists or cybercriminals seeking to tap into sensor data transmissions or to cause mayhem by hacking or jamming command and control signals.

Terrorists could potentially use drones to carry out small-scale attacks using explosives, or as platforms for chemical, biological, or radiological attacks. In September 2011, the FBI disrupted a homegrown terrorist plot to attack the Pentagon and the Capitol with large model aircraft packed with high explosives. The incident heightened concern about potential terrorist attacks using unmanned aircraft. Widely publicized drone incidents, including an unauthorized flight at a political rally in Dresden, Germany, in September 2013 that came in close proximity to German Chancellor Angela Merkel; a January 2015 crash of a small hobby drone on the White House lawn in Washington, DC; and a series of unidentified drone flights over landmarks and sensitive locations in Paris, France, in 2015, have raised additional concerns about security threats posed by small unmanned aircraft. Recently, the use of drones, including weaponized drones, by IS has renewed fears that unmanned aircraft may be utilized in a terrorist attack.[203] Domestically, there have been numerous reports of drones flying in close proximity to airports and manned aircraft, in restricted airspace, and over stadiums and outdoor events. The payload capacities of small unmanned aircraft would limit the damage a terrorist attack using conventional explosives could inflict, but drone attacks using chemical, biological, or radiological weapons could be more serious.

FAA regulations require TSA to carry out threat assessments of commercial UAS operators, as it does for civilian pilots.[204] However, this requirement does not apply to recreational users, although they must register with FAA. Moreover, while FAA has issued general guidance to law enforcement regarding unlawful UAS operations,[205] it is not clear that law enforcement agencies have sufficient training or technical capacity to respond to this emerging threat.[206]

---

[203] Joby Warrick, "Use of Weaponized Drones by ISIS Spurs Terrorism Fears," *Washington Post*, February 21, 2017.

[204] Federal Aviation Administration, "Operation and Certification of Small Unmanned Aircraft Systems; Final Rule," 81 *Federal Register* 42064-42214, June 28, 2016.

[205] Federal Aviation Administration, *Law Enforcement Guidance for Suspected Unauthorized UAS Operations*, http://www.faa.gov/uas/regulations_policies/media/FAA_UAS-PO_LEA_Guidance.pdf.

[206] Statement of Chief Richard Beary, President of the International Association of Chiefs of Police, Subcommittee on Oversight and Management Efficiency, Committee on Homeland Security, U.S. House of Representatives, March 18, (continued...)

Technology may help manage security threats posed by unmanned aircraft. Integrating tracking mechanisms as well as incorporating "geo-fencing" capabilities, designed to prevent flights over sensitive locations or in excess of certain altitude limits, into unmanned aircraft systems may help curtail unauthorized flights.[207]

While unmanned aircraft may pose security risks, they are also a potential asset for homeland security operations, particularly for CBP border surveillance. CBP currently employs a fleet of nine modified Predator UASs. Operating within specially designated airspace, these unarmed UASs patrol the northern and southern land borders and the Gulf of Mexico to detect potential border violations and monitor suspected drug trafficking, with UAS operators cuing manned responses when appropriate. State and local governments have expressed interest in operating UASs for missions as diverse as traffic patrol, surveillance, and event security. A small but growing number of state and local agencies have acquired drones, some through federal grant programs, and have been issued special authorizations by FAA to fly them. However, many federal, state, and local agencies involved in law enforcement and homeland security appear to be awaiting more specific guidance from FAA regarding the routine operation of public-use unmanned aircraft in domestic airspace.

The introduction of drones into domestic surveillance operations presents a host of novel legal issues related to an individual's fundamental privacy interest protected under the Fourth Amendment.[208] Several measures introduced in Congress would require government agents to obtain warrants before using drones for domestic surveillance, but would create exceptions for patrols of the national borders used to prevent or deter illegal entry and for investigations of credible terrorist threats.[209]

Language in P.L. 114-190 directs FAA to establish a pilot program to detect and mitigate unmanned aircraft operations in the vicinity of airports and other critical infrastructure. Additionally, the act directs FAA to develop an air traffic management system for small UASs that, in addition to addressing safety concerns, could include measures to detect and deter security threats posed by UASs.

FAA separately addresses cybersecurity of government-owned air traffic control systems and certified aircraft systems. However, GAO has cautioned that FAA's current approach to cybersecurity does not adequately address the interdependencies between aircraft and air traffic systems, and consequently may hinder efforts to develop a comprehensive and coordinated strategy.[210] While it identified no easy fix, GAO recommended that FAA develop a comprehensive cybersecurity threat model, better clarify cybersecurity roles and responsibilities, improve management security controls and contractor oversight, and fully incorporate National Institute of Standards and Technology information security guidance throughout the system life cycle.

(...continued)

2015.

[207] See, e.g., Todd Humphreys, "Statement on the Security Threat Posed by Unmanned Aerial Systems and Possible Countermeasures," Submitted to the Subcommittee on Oversight and Management Efficiency, House Committee on Homeland Security, March 16, 2015.

[208] See CRS Report R42701, *Drones in Domestic Surveillance Operations: Fourth Amendment Implications and Legislative Responses*, by Richard M. Thompson II.

[209] See, e.g., H.R. 1229, H.R. 1385, S. 635.

[210] Government Accountability Office, *Air Traffic Control: FAA Needs a More Comprehensive Approach to Address Cybersecurity As Agency Transitions to NextGen*, GAO-15-370, April 2015.

Language in P.L. 114-190 mandates development of a comprehensive strategic framework for reducing cybersecurity risks to the national airspace system, civilian aviation, and FAA information systems. The framework is to address cybersecurity risks associated with airspace modernization, aircraft automation, and in-flight entertainment systems. The act also directs FAA to assess the cost and schedule for developing and maintaining an agency-wide cybersecurity threat model as recommended by GAO, and produce a standards plan to implement security guidance for FAA data and information systems.

Transit and Passenger Rail Security

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

Bombings of and shootings on passenger trains in Europe and Asia have illustrated the vulnerability of passenger rail systems to terrorist attacks. Passenger rail systems—primarily subway systems—in the United States carry about five times as many passengers each day as do airlines, over many thousands of miles of track, serving stations that are designed primarily for easy access. The increased security efforts around air travel have led to concerns that terrorists may turn their attention to "softer" targets, such as transit or passenger rail. A key challenge Congress faces is balancing the desire for increased rail passenger security with the efficient functioning of transit systems, with the potential costs and damages of an attack, and with other federal priorities.

The volume of ridership and number of access points make it impractical to subject all rail passengers to the type of screening all airline passengers undergo. Consequently, transit security measures tend to emphasize managing the consequences of an attack. Nevertheless, steps have been taken to try to reduce the risks, as well as the consequences, of an attack. These include vulnerability assessments; emergency planning; emergency response training and drilling of transit personnel (ideally in coordination with police, fire, and emergency medical personnel); increasing the number of transit security personnel; installing video surveillance equipment in vehicles and stations; and conducting random inspections of bags, platforms, and trains.

The challenges of securing rail passengers are dwarfed by the challenge of securing bus passengers. There are some 76,000 buses carrying 19 million passengers each weekday in the United States. Some transit systems have installed video cameras on their buses, but the number and operating characteristics of transit buses make them all but impossible to secure.

In contrast with the aviation sector, where TSA provides security directly, security in surface transportation is provided primarily by the transit and rail operators and local law enforcement agencies. TSA's role is one of oversight, coordination, intelligence sharing, training, and assistance, though it does provide some operational support through its Visible Intermodal Prevention and Response (VIPR) teams, which conduct operations with local law enforcement officials, including periodic patrols of transit and passenger rail systems to create "unpredictable visual deterrents."

The Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L. 110-53), passed by Congress on July 27, 2007, included provisions on passenger rail and transit security and authorized $3.5 billion for FY2008-FY2011 for grants for public transportation security. The act required public transportation agencies and railroads considered to be high-risk targets by DHS to have security plans approved by DHS (§1405 and §1512). Other provisions required DHS to conduct a name-based security background check and an immigration status check on all public transportation and railroad frontline employees (§1414 and §1522), and gave DHS the authority to regulate rail and transit employee security training standards (§1408 and §1517).

In 2010 TSA completed a national threat assessment for transit and passenger rail, and in 2011 completed an updated transportation systems sector-specific plan, which established goals and objectives for a secure transportation system. The three primary objectives for reducing risk in transit are

- increase system resilience by protecting high-risk/high-consequence assets (e.g., critical tunnels, stations, and bridges);
- expand visible deterrence activities (e.g., canine teams, passenger screening teams, and antiterrorism teams); and
- engage the public and transit operators in the counterterrorism mission.[211]

TSA surface transportation security inspectors conduct assessments of transit systems (and other surface modes) through the agency's Baseline Assessment for Security Enhancement (BASE) program. The agency has also developed a security training and security exercise program for transit (I-STEP).

The House Committee on Homeland Security's Subcommittee on Transportation Security held a hearing in May 2012 to examine the surface transportation security inspector program. The number of inspectors had increased from 175 full-time equivalents in FY2008 to 404 in FY2011. Issues considered at the hearing included the lack of surface transportation expertise among the inspectors, many of whom were promoted from screening passengers at airports; the administrative challenge of having the surface inspectors managed by federal security directors who are located at airports and who themselves typically have no surface transportation experience; and the security value of the tasks performed by surface inspectors.[212] The number of surface inspectors decreased to 260 (full-time equivalent positions) in FY2016, in part reflecting a reduction in the number of VIPR surface inspectors and in part reflecting efficiencies achieved through focusing efforts on the basis of risk.[213]

GAO reported in 2014 that lack of guidance to TSA's surface inspectors resulted in inconsistent reporting of rail security incidents and that TSA had not consistently enforced the requirement that rail agencies report security incidents, resulting in poor data on the number and types of incidents.[214] GAO also found that TSA did not have a systematic process for collecting and addressing feedback from surface transportation stakeholders regarding the effectiveness of its information-sharing effort.[215] In a 2015 hearing, GAO testified that TSA has put processes in place to address these issues.[216]

---

[211] Department of Homeland Security, Transportation Security Administration, *Surface Transportation Security FY2016 Congressional [Budget] Justification*, p. 11.

[212] U.S. House of Representatives, Committee on Homeland Security, Subcommittee on Transportation Security, Hearing on *TSA's Surface Inspection Program: Strengthening Security or Squandering Resources?*, May 31, 2012, http://homeland.house.gov/hearing/subcommittee-hearing-tsa%E2%80%99s-surface-inspection-program-strengthening-security-or-squandering.

[213] Peter Neffenger, Administrator, Transportation Security Administration, U.S. Department of Homeland Security, *Statement to the United States Senate Committee on Commerce, Science, and Transportation*, Hearing on Transportation Security, April 6, 2016; Department of Homeland Security, Transportation Security Administration, *Surface Transportation Security FY2014 Congressional [Budget] Justification*, p. 14.

[214] Government Accountability Office, *Passenger Rail Security: Consistent Incident Reporting and Analysis Needed to Achieve Program Objectives*, GAO-13-20, December 19, 2012.

[215] Government Accountability Office, *Transportation Security Information Sharing: Stakeholder Satisfaction Varies; TSA Could Take Additional Actions to Strengthen Efforts*, GAO-14-506, June 24, 2014.

[216] Government Accountability Office, *Surface Transportation Security: TSA Has Taken Steps Designed to Develop Process for Sharing and Analyzing Information and to Improve Rail Security Incident Reporting*, GAO-15-205T, given (continued...)

DHS provides grants for security improvements for public transit, passenger rail, and occasionally other surface transportation modes under the Transit Security Grant Program. The vast majority of the funding goes to public transit providers. CRS estimates that, on an inflation-adjusted basis, funding for this program has declined 84% since 2009, when Congress allocated $150 million in the American Recovery and Reinvestment Act, in addition to routine appropriations.

In a February 2012 report, GAO found potential for duplication among four DHS state and local security grant programs with similar goals, one of which was the public transportation security grant program.[217] The Obama Administration proposed consolidating several of these programs in the annual budget requests for FY2013 through FY2016. This proposal was not supported by Congress at the time.

In P.L. 114-50, Congress directed TSA to ensure that all passenger transportation providers it considers as having high-risk facilities have in place plans to respond to active shooters, acts of terrorism, or other security-related incidents that target passengers.

Disaster Preparedness, Response, and Recovery

Disaster Assistance Funding

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

For further information, see CRS Report R43537, *FEMA's Disaster Relief Fund: Overview and Selected Issues*, by Bruce R. Lindsay and CRS Report R42352, *An Examination of Federal Disaster Relief Under the Budget Control Act*, by Bruce R. Lindsay, William L. Painter, and Francis X. McCarthy

The majority of disaster assistance provided by the Federal Emergency Management Agency (FEMA) to states and localities after a declared emergency or major disaster is funded with monies from the Disaster Relief Fund (DRF).[218]

In general, Congress annually appropriates budget authority to the DRF to ensure that funding is available for recovery projects from previous incidents (some of these projects take several years to complete) and to create a reserve to pay for emergencies and major disasters that might occur that fiscal year. Any remaining balance in the DRF at the end of the fiscal year is carried over to the next fiscal year.

Because of the unpredictable nature of disasters and competing demands in the discretionary budget, normal annual appropriations have often not always adequately funded the DRF. From FY2004 to FY2013 Congress provided additional budget authority for the DRF through supplemental appropriations fourteen times.[219] This reliance on emergency supplemental

(...continued)

before the U.S. House of Representatives, Committee on Homeland Security, Subcommittees on Transportation Security and Counterterrorism and Intelligence, September 17, 2015.

[217] United States Governmental Accountability Office, *Homeland Security: DHS Needs Better Project Information and Coordination among Four Overlapping Grant Programs*, GAO-12-303, February 2012.

[218] For further analysis on emergency and major disaster declarations see CRS Report R43784, *FEMA's Disaster Declaration Process: A Primer*, by Francis X. McCarthy. For more information on the Disaster Relief Fund see CRS Report R43537, *FEMA's Disaster Relief Fund: Overview and Selected Issues*, by Bruce R. Lindsay.

[219] For information on supplemental appropriations for disasters see CRS Report R43665, *Supplemental Appropriations* (continued...)

appropriations has been of particular congressional concern. In addition, the number of disasters being declared over the last two decades has risen, as have their costs.[220] The upward trend in federal disaster costs have periodically reopened discussions of how to control, reduce, or offset[221] federal spending on major disasters.

Prior to the passage of the Budget Control Act in 2011 (BCA, P.L. 112-25), supplemental appropriations for disasters were often designated as an emergency expenditure, which under congressional budgetary procedures can exceed discretionary spending limits. Congress included provisions on disaster relief spending when it passed the BCA. The BCA sets overall discretionary spending caps and provides two types of adjustments that could be applied to make room for disaster assistance—a limited adjustment specifically for the costs of major disasters under the Stafford Act,[222] and an unlimited adjustment for more broadly defined emergency spending.

The proportion of DRF funding provided in annual appropriations legislation has grown since the passage of the BCA, and emergency funding for the DRF has been provided in supplemental appropriations legislation only once since FY2012, in response to Hurricane Sandy.[223] It could be argued that catastrophic events such as Hurricane Sandy still represent a challenge to those who wish to reduce or eliminate emergency designations for disaster relief funding.

Another potential challenge concerns how the allowable adjustment is calculated. The budgetary exemption for the cost of major disasters has been declining as a result of the way the formula is calculated, which does not capture the total federal costs of responding to and recovering from disasters. This increases the likelihood that Congress may again face the decision of whether to provide emergency funding for the DRF in the wake of disasters of a less catastrophic degree.[224]

The amount of money the federal government provides for disaster relief has been of congressional concern, particularly in recent years. While some might argue the expenditures are justified because they provide important assistance to states and localities, others may be interested in finding ways to reduce federal costs.

With respect to the decline in the allowable adjustment for the cost of major disasters, Congress could choose to continue to use emergency funding to meet unbudgeted disaster relief needs, or explore changes to the allowable adjustment's underlying calculation that would increase it—and thus reduce the need for emergency funding.

(...continued)

for Disaster Assistance: Summary Data and Analysis, by Bruce R. Lindsay and Justin Murray.

[220] For further analysis on Stafford Act declarations from 1953 to 2015 see CRS Report R42702, *Stafford Act Declarations 1953-2015: Trends, Analyses, and Implications for Congress*, by Bruce R. Lindsay and Francis X. McCarthy.

[221] Congress has only offset supplemental funding for the DRF once, through a coincidental combination of legislation. For more details, see CRS Report R42458, *Offsets, Supplemental Appropriations, and the Disaster Relief Fund: FY1990-FY2013*, by William L. Painter.

[222] The adjustment limitation is not a restriction on disaster assistance—it is a restriction on how much the discretionary budget cap can be adjusted upward by that particular mechanism to accommodate the assistance.

[223] For further analysis on disaster assistance under the Budget Control Act see CRS Report R42352, *An Examination of Federal Disaster Relief Under the Budget Control Act*, by Bruce R. Lindsay, William L. Painter, and Francis X. McCarthy

[224] For more in-depth discussion on the reduction in the 10-year average see CRS Report R44415, *Five Years of the Budget Control Act's Disaster Relief Adjustment*, coordinated by William L. Painter.

The allowable adjustment expires by existing law at the beginning of FY2022. Congress may choose to begin considering utility of the disaster relief adjustment and the effect it has had on federal disaster assistance.

Firefighter Assistance Programs

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

For further information, see CRS Report RL32341, *Assistance to Firefighters Program: Distribution of Fire Grant Funding*, and CRS Report RL33375, *Staffing for Adequate Fire and Emergency Response: The SAFER Grant Program*.

Although firefighting activities are traditionally the responsibility of states and local communities, Congress has established federal firefighter assistance grant programs within DHS to provide additional support for local fire departments. In 2000, the 106th Congress established the Assistance to Firefighters Grant Program (AFG), which provides grants to local fire departments for firefighting equipment and training. In the wake of the 9/11 attacks, the scope and funding for AFG were expanded. Additionally in 2003, the 108th Congress established the Staffing for Adequate Fire and Emergency Response (SAFER) program, which provides grants to support firefighter staffing.

In the 115th Congress, debate over firefighter assistance programs is likely to take place within the appropriations and reauthorization process. With respect to annual appropriations, arriving at funding levels for AFG and SAFER is subject to two countervailing considerations. On the one hand, what fire grant supporters view as inadequate state and local public safety budgets have led them to argue for the necessity of maintaining, if not increasing, federal grant support for fire departments. On the other hand, concerns over reducing overall federal discretionary spending and the appropriateness of federal support for local firefighting have led others to question whether continued or reduced federal support for AFG and SAFER is warranted.

Authorization for AFG and SAFER expires on September 30, 2017, and the 115th Congress may consider reauthorization legislation. Historically, debate over the firefighter assistance reauthorization has reflected a competition for funding between career/urban/suburban departments and volunteer/rural departments. The continuing issue is how 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.

Emergency Communications

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

For further information, see CRS Report R42543, *The First Responder Network (FirstNet) and Next-Generation Communications for Public Safety: Issues for Congress*, by Lennard G. Kruger.

Emergency communications systems support first responders and other emergency personnel, disseminate alerts and warnings to residents in endangered areas, and relay calls for help through 911 call networks. These networks support day-to-day needs to protect the safety of the public and deliver critical information before, during, and after disasters.

The technologies that support emergency communications are converging toward a common platform using the Internet Protocol (IP). Federal, state, and local agencies are investing in IP-enabled communications infrastructure that can be shared to support all forms of emergency communications. Notable examples of new investment include

- interoperable public safety communications networks;
- digital alerts and warnings; and
- Next Generation 9-1-1 (NG 9-1-1) networks.

The 115th Congress is likely to continue overseeing the federal programs that have been established to promote and support emergency communications systems. Notable federal programs are the First Responder Network Authority (FirstNet);[225] the Integrated Public Alert and Warning System (IPAWS);[226] and the National 9-1-1 Program.[227] FirstNet is an independent authority established within the National Telecommunications and Information Administration (NTIA) to develop a nationwide broadband network for emergency communications. IPAWS alert and warning capabilities are coordinated through the Federal Emergency Management Agency with the participation of the Federal Communications Commission. The activities of the National 9-1-1 Program, which focus on providing a base for improving 9-1-1 infrastructure, are conducted jointly by the National Highway Traffic Safety Administration and the NTIA.

Coordination of these discrete programs is assisted by federal programs and guidance described in the DHS *National Emergency Communications Plan*.[228] The Homeland Security Act of 2002 (P.L. 107-296), Title XVIII, as amended, directs the DHS Office of Emergency Communications (OEC) to develop and periodically update a plan in consultation with federal, state, local, tribal, territorial, and private sector stakeholders. Currently, the OEC is developing the Nationwide Communications Baseline Assessment (NCBA) to evaluate the nation's ability to communicate during a response to routine incidents, natural disasters, acts of terrorism, and other man-made disasters.[229]

The *National Emergency Communications Plan* recognizes the advantages of converging emergency communications platforms and coordinating across federal, state, local, and tribal agencies. The plan identifies four categories of emergency response that in time should converge. These are: communications for incident response and coordination; notifications, alerts, and warnings; public information exchange; and requests for assistance and reporting. The top three priorities for the plan over the three to five years following publication are identifying and prioritizing areas for improvement in emergency responders' narrowband networks (Land Mobile Radio, or LMR); facilitating the adoption, integration, and use of broadband technologies, notably the broadband network to be deployed by FirstNet; and enhancing coordination among stakeholders across the emergency response community.

[225] Information on FirstNet is available at http://www.firstnet.gov.

[226] Information on IPAWS is available at https://www.fema.gov/integrated-public-alert-warning-system.

[227] Established as the 9-1-1 Implementation Coordination Office (ICO) by Congress in 2004 and reauthorized by P.L. 112-96; see 47 U.S.C. §942. Information on the National 9-1-1 Program is available at https://www.911.gov.

[228] *National Emergency Communications Plan*, 2014, available at http://www.dhs.gov/sites/default/files/publications/2014%20National%20Emergency%20Communications%20Plan_October%2029%202014.pdf.

[229] Department of Homeland Security, Office of Emergency Communications, Nationwide Communications Baseline Assessment, September 2016, available at https://www.dhs.gov/sites/default/files/publications/NCBA%20Factsheet_September%202016_FINAL%20508C.pdf.

The National Flood Insurance Program (NFIP)

Diane P. Horn, Analyst in Flood Insurance and Emergency Management (dhorn@crs.loc.gov, 7-3472)

For further information, see CRS Report R44593, *Introduction to the National Flood Insurance Program (NFIP)*, by Diane P. Horn and Jared T. Brown.

The National Flood Insurance Program (NFIP) was established by the National Flood Insurance Act of 1968 (NFIA, 42 U.S.C. §4001 et seq.) and was most recently reauthorized by the Biggert-Waters Flood Insurance Reform Act of 2012 (BW-12, Title II of P.L. 112-141). The general purpose of the NFIP is both to offer primary flood insurance to properties with significant flood risk, and to reduce flood risk through the adoption of floodplain management standards. A longer term objective of the NFIP is to reduce federal expenditure on disaster assistance after floods. The NFIP is managed by the Federal Emergency Management Agency (FEMA), through its subcomponent Federal Insurance and Mitigation Administration (FIMA). Currently 22,233 communities participate in the NFIP, with over five million policies in force and over $1.2 trillion in coverage.[230] According to FEMA, the program saves the nation an estimated $1.87 billion annually in flood losses avoided because of the NFIP's building and floodplain management regulations.[231] Floods are the most common natural disaster in the U.S. and in recent years all fifty states have experienced flood events.[232] U.S. flood losses in 2016 were about $17 billion, which was six times greater than the overall flood damage in 2015, with losses from five flood-related events in 2016 exceeding $1 billion.[233]

Congress amended elements of BW-12, but did not extend the NFIP's authorization further in the Homeowner Flood Insurance Affordability Act of 2014 (HFIAA-14, P.L. 113-89). 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, 2017:

- The authority to provide *new* flood insurance contracts will expire.[234] Flood insurance contracts entered into before the expiration would continue until the end of their policy term of one year.
- The authority for NFIP to borrow funds from the Treasury will be reduced from $30.425 billion to $1.5 billion.[235]
- The authorization of appropriations for the flood hazard mapping program will expire. This program could continue, subject to appropriations, beyond this date.[236]

[230] Statistics on the NFIP policy and claims are available from FEMA's website at https://www.fema.gov/policy-claim-statistics-flood-insurance.

[231] Ibid.

[232] See the NFIP FloodSmart website at https://www.floodsmart.gov/floodsmart/pages/flood_facts.jsp.

[233] CoreLogic, *2016 Natural Hazard Risk Summary and Analysis*, January 26, 2017, http://www.corelogic.com/about-us/researchtrends/natural-hazard-risk-summary-and-analysis.aspx?WT.mc_id=crlg_170126_VVDR4&elqTrackId=2d592d1bfe03491b9cb6a931f3eb4b97&elq=402cd8257b39479fb09d77e2338b2f6d&elqaid=12063&elqat=1&elqCampaignId=5207#.

[234] 42 U.S.C. §4026.

[235] 42 U.S.C. §4016(a).

[236] 42 U.S.C. §4104b(f).

Other activities of the program would technically remain authorized following September 30, 2017, such as the issuance of FMA grants.[237] However, the expiration of the key authorities described above would have varied and generally serious effects on these remaining NFIP activities.

Issues which the 115th Congress may consider as part of the reauthorization of the NFIP include

- NFIP debt and borrowing,
- affordability and solvency, and
- the role of private insurance in the NFIP.

NFIP Debt and Borrowing

Congress has authorized FEMA to borrow no more than $30.425 billion from the U.S. Treasury in order to operate the NFIP. Prior to the 2005 hurricane season, the NFIP had generally been able to cover its costs, borrowing relatively small amounts from the U.S. Treasury to pay claims, and then repaying the loans with interests. The NFIP was forced to borrow heavily to pay claims in the aftermath of the 2005 hurricane season (Hurricanes Katrina, Rita, and Wilma) and Hurricane Sandy in 2012.[238] Following Hurricane Sandy, Congress passed P.L. 113-1 to increase the borrowing limit of the NFIP from $20.775 billion to the current $30.425 billion. A reserve fund assessment was authorized by Congress in BW-12 to establish and maintain a Reserve Fund to cover future claim and debt expenses, especially those from catastrophic disasters.[239] In addition to the reserve fund assessment, all NFIP policies are also being assessed a surcharge following the passage of HFIAA.[240] However, despite these additional sources of income, in January 2017 the NFIP borrowed an additional $1.6 billion to cover incurred losses in 2016 and anticipated programmatic activities. FEMA's view is that "even if losses are somewhat favorable over an extended period, the NFIP will still not come close to repaying the debt."[241] As of March 31, 2017, the NFIP owed $24.6 billion in debt to the U.S. Treasury, leaving $5.825 billion left in available borrowing authority, and FIMA had $1.266 billion available ($819 million in the National Flood Insurance Fund and $447 million in the Reserve Fund).[242] Under its current authorization, the only means the NFIP has to pay off the debt is through the accrual of premium revenues in excess of outgoing claims, and from payments from the Reserve Fund. Congress may consider additional sources of funding or whether to forgive all or part of the existing debt.[243]

Affordability and Solvency

As a public insurance program, the goals of the NFIP are very different from the goals of private sector companies, as it encompasses social goals to provide flood insurance in flood-prone areas to property owners who otherwise would not be able to obtain it and reduce government's cost

[237] See 42 U.S.C. §4104c and 42 U.S.C. §4104d.

[238] For accounting of the NFIP's premium revenues and claims/loss data, see FEMA's website for policy and claim statistics at https://www.fema.gov/policy-claim-statistics-flood-insurance.

[239] Section 100212 of P.L. 112-141, 126 Stat. 992, as codified at 42 U.S.C. §4017a.

[240] Section 8(a) of P.L. 113-89, 128 Stat. 1023.

[241] Email correspondence from FEMA Congressional Affairs staff, quoting Roy E. Wright, FEMA's Deputy Associate Administrator for Insurance and Mitigation, March 17, 2017.

[242] Email correspondence from FEMA Congressional Affairs staff, April 18, 2017.

[243] For example, H.R. 5953 was introduced in the House in the 114th Congress to forgive the indebtedness of the NFIP. It was referred to the House Budget Committee on September 8, 2016.

after floods.[244] Congress has expressed concern related to the perceived affordability of flood insurance premiums and the balance between actuarial soundness and other goals of the NFIP. In BW-12, Congress required FEMA to commission a study with the National Academy of Sciences (NAS) regarding participation in the NFIP and the affordability of premiums, which was published report in two parts.[245] In HFIAA-14, Congress also required FEMA to develop a Draft Affordability Framework "that proposes to address, via programmatic and regulatory changes, the issues of affordability of flood insurance sold under the National Flood Insurance Program, including issues identified in the affordability study…."[246] Due 18 months following the submission of the Affordability Study, FEMA has not yet submitted the Framework. The deadline for the Framework, based on FEMA stated date of submittal of the Affordability Study, is September 10, 2017.[247] Congress may consider how to define 'affordability' and how it might be achieved.

The Role of Private Insurance in the NFIP

The role of the private insurance industry in the flood insurance market is likely to be a major consideration in the reauthorization of the NFIP. Currently, while FEMA provides the overarching management and oversight of the NFIP, the bulk of the day-to-day operation of the NFIP, including the marketing, sale, writing, and claims management of policies, is handled by private companies. This arrangement between the NFIP and private industry is authorized by statute and guided by regulation.[248] There are two different arrangements that FEMA has established with private industry. The first is the Direct Servicing Agent, or DSA, which operates as a private contractor on behalf of FEMA for individuals seeking to purchase flood insurance policies directly from the NFIP.[249] The second arrangement is called the Write-Your-Own (WYO) Program, where private insurance companies are paid to directly write and service the policies themselves. With either the DSA or WYO Program, the NFIP retains the actual financial risk of paying claims for the policy (i.e., underwrites the policy), and the policy terms and premiums are the same. Roughly 86% of NFIP policies are sold by the over 70 companies participating the WYO Program.[250]

A number of private insurance companies and insurance industry organizations have expressed interest in private insurers offering primary flood insurance in competition with the NFIP. This would present a number of issues which Congress would need to consider, many of which were

[244] See 82 Stat. 573 for text in original statute (Section 1302(c) of P.L. 90-448). This language remains in statute (see 42 U.S.C. §4001(c)).

[245] See National Research Council of the National Academies, *Affordability of National Flood Insurance Program Premiums: Report 1*, 2015, at http://www.nap.edu/catalog/21709/affordability-of-national-flood-insurance-program-premiums-report-1; and National Research Council of the National Academies, *Affordability of National Flood Insurance Program Premiums: Report 2*, 2016, at http://www.nap.edu/catalog/21848/affordability-of-national-flood-insurance-program-premiums-report-2.

[246] Section 9(a) of P.L. 113-89, 128 Stat. 1024.

[247] Section 9(c) of P.L. 113-89, 128 Stat. 1024. FEMA has stated it officially submitted the Affordability Study on March 10, 2016 (email correspondence with FEMA Congressional Affairs staff, March 10, 2016). However, Part 2 of the Affordability Study was available from the NAS website on December 11, 2015.

[248] See primarily 42 U.S.C. §4081 and §4018, and 44 C.F.R. Part 62.

[249] The current Direct Servicing Agent is a company called National Flood Services, and they operate website at https://www.nfipservices.com/.

[250] Email correspondence from FEMA Congressional Affairs staff, July 18, 2016. A list of companies participating in the WYO Program is available at https://www.fema.gov/wyo_company.

discussed in FEMA's report to Congress[251] required by BW-12.[252] Particular challenges identified by the report include how to maintain the funding of federal flood mapping and floodplain management activities, which are currently funded through the Federal Policy Fee charged on all flood insurance policies,[253] and how to ensure the affordability and continued availability of flood insurance to property owners in flood zones. If private insurance companies enter the market in larger numbers, should they be expected to contribute to the cost of mapping and floodplain management? If so, how might this be addressed? How might private companies be prevented from "cherry-picking" (i.e., adversely selecting) the profitable, lower-risk policies and leaving the NFIP with the high-risk, actuarially unsound policies?

FEMA Reauthorization

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

FEMA has several important authorizing statutes that arguably have not been comprehensively reauthorized in recent Congresses.[254] These statutes include, but are not limited to, the Robert T. Stafford Disaster Relief and Emergency Assistance Act (P.L. 93-288, as amended, 42 U.S.C. §5121 et seq., henceforth the Stafford Act), the Homeland Security Act of 2002 (P.L. 107-296, as amended, 6 U.S.C. §101 et seq., henceforth HSA 2002), and the National Flood Insurance Act of 1968 (P.L. 90-488, as amended, 42 U.S.C. §4001 et seq., henceforth the NFIA). While only the NFIA has significant authorities that will expire during the 115th Congress and require reauthorization,[255] the 115th Congress may also seek to reauthorize and reform multiple provisions of the Stafford Act or the HSA 2002. Such revisions have been considered in recent past Congresses but were not enacted into law. For instance, in the 114th Congress, the House passed H.R. 1471, the FEMA Disaster Assistance Reform Act of 2015, which included numerous provisions revising authorities of the Stafford Act. While the Senate passed portions of this bill separately, to include the ultimate passage into law of a reauthorization for FEMA's Urban Search and Rescue System (P.L. 114-326), most other provisions of the bill were not enacted in both chambers.

There are many, varied options the 115th Congress could consider when looking at either the FEMA-related provisions of either the HSA 2002 or Stafford Act. Such legislative action could be pursued in response to a major future incident, as was the case for Hurricanes Sandy and Katrina, which provokes concerns in Congress regarding the sufficiency of FEMA's existing authorization. Alternatively, such legislative action could be pursued in conjunction with a likely debate on the reauthorization of the NFIA in the 115th Congress. As hypothetical examples, the 115th Congress could decide to

---

[251] Federal Emergency Management Agency, *National Flood Insurance Program Report to Congress on Reinsuring NFIP Insurance Risk and Options for Privatizing the NFIP*, August 13, 2015, http://www.floods.org/ace-files/documentlibrary/2012_NFIP_Reform/Reinsuring_NFIP_Insurance_Risk_and_Options_for_Privatizing_the_NFIP_Report.pdf.

[252] Section 100232(a) of P.L. 112-141.

[253] 42 U.S.C. §4014(a)(1)(B)(iii).

[254] Identifying 'reauthorizations' can be subjective; one might suggest that the last major reauthorization of Stafford Act provisions was passed into law following Hurricane Sandy in the Sandy Recovery Improvement Act (Division B of P.L. 113-2, the Disaster Relief Appropriations Act, 2013), while the last major reauthorization of the FEMA-related provisions of the HSA 2002 came in the Post-Katrina Emergency Reform Act of 2006 (Title VI of P.L. 109-295, the Department of Homeland Security Appropriations Act, 2007).

[255] For more on the reauthorization of the NFIA and NFIP, see "The National Flood Insurance Program (NFIP)."

- limit or expand the forms of federal disaster assistance provided by FEMA through the Stafford Act,[256]
- reauthorize the predisaster hazard mitigation (PDM) program and its authorization of appropriations in the Stafford Act,[257]
- revise the Administrator's authorities related to the broader homeland security mission in the HSA 2002,[258] or
- reauthorize the appropriations for the administration of FEMA in HSA 2002, as amended by the Post-Katrina Emergency Management Reform Act (PKEMRA).[259]

National Preparedness System

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

The United States is threatened by a wide array of hazards, including natural disasters, acts of terrorism, viral pandemics, and manmade disasters such as the Deepwater Horizon oil spill. The way the nation strategically prioritizes and allocates resources to prepare for hazards can significantly influence the ultimate cost to society, both in the number of human casualties and the scope of economic damage. Subtitle C of the Post-Katrina Emergency Reform Act of 2006 (PKEMRA; P.L. 109-295, 6 U.S.C. §741-764) requires the President, acting through the Administrator of FEMA, 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."[260]

Currently, the creation of a NPG and NPS is guided by Presidential Policy Directive 8: National Preparedness (PPD-8), issued by then-President Barack Obama on March 30, 2011.[261] PPD-8 rescinded the existing Homeland Security Presidential Directive 8: National Preparedness (HSPD-8),[262] 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).[263] In brief, the NPS and its many component policies embody the strategic vision and planning of the federal government, with input from the *whole community*,[264] as it relates to preparing the nation for all

[256] See, for example, Sections 403, 404, 406, 408, and 428 of the Stafford Act (42 U.S.C. §§5170b, 5170c, 5172, 5174, 5189f).

[257] See Section 203(m) of the Stafford Act (42 U.S.C. §5133).

[258] See, for example, Section 504 of HSA 2002 (6 U.S.C. §314).

[259] 6 U.S.C. §811.

[260] 6 U.S.C. §§743-744.

[261] White House, *Presidential Policy Directive 8: National Preparedness*, Washington, DC, March 30, 2011, p. 1, http://www.dhs.gov/xabout/laws/gc_1215444247124.shtm.

[262] White House, *Homeland Security Policy Directive 8: National Preparedness*, Washington, DC, December 17, 2003. http://www.dhs.gov/files/publications/gc_1189788256647.shtm. Hereafter, the document will be referenced in footnotes as HSPD-8.

[263] For a summary listing of major component policies, see FEMA's website at https://www.fema.gov/learn-about-presidential-policy-directive-8.

[264] The "whole community" includes individuals and families, including those with access and functional needs; (continued...)

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*[265] necessary to achieve the NPG. Furthermore, the NPS includes annual National Preparedness Reports that serve as pseudo report cards on progress being made toward achieving national preparedness objectives.[266] The Reports rely heavily on a self-assessment process, called the Threat and Hazard Identification and Risk Assessment (THIRA), to incorporate the perceived risks and capabilities of the whole community into the national preparedness system (NPS).[267] 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.

The 115th Congress may continue its oversight of the NPS. It is within the discretion of the Administration to retain, revise, or replace the overarching guidance of PPD-8. In either case, Congress may have interest in overseeing the NPS on a variety of factors, such as whether

- the NPS conforms to the objectives of Congress, as outlined in the PKEMRA statute;
- federal roles and responsibilities have, in the opinion of Congress, 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 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 115th Congress, Congress could consider amending the PKEMRA statute to create new requirements, or revising existing provisions, to manage the amount of discretion afforded to the President in creating the NPS. This could mean, for example, the 115th Congress directly assigning certain preparedness responsibilities to federal agencies through authorizing legislation different than those indicated

(...continued)

businesses; faith-based and community organizations; nonprofit groups; schools and academia; media outlets; and all levels of government, including state, local, tribal, territorial, and federal partners. See more at FEMA's website at http://www.fema.gov/national-preparedness/whole-community.

[265] 6 U.S.C. 741(1) defines *capability* 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 one that is "necessary to prepare for the specific types of incidents that pose the greatest risk to the security of the Nation." See White House, *Presidential Policy Directive 8: National Preparedness*, Washington, DC, March 30, 2011, p. 2, http://www.dhs.gov/xabout/laws/gc_1215444247124.shtm.

[266] As of the date of publication of this CRS report, the latest version of the National Preparedness Report summarizes activities through CY2015. See Department of Homeland Security, *National Preparedness Report*, March 30, 2016, at https://www.fema.gov/media-library/assets/documents/116951.

[267] For more on THIRA, see FEMA's website on the topic at https://www.fema.gov/threat-and-hazard-identification-and-risk-assessment and Department of Homeland Security, *Threat and Hazard Indentification and Risk Assessment Guide, Comprehensive Preparedness Guide (CPG) 201*, Second Edition, August 2013, at https://www.fema.gov/media-library-data/8ca0a9e54dc8b037a55b402b2a269e94/CPG201_htirag_2nd_edition.pdf.

by national preparedness frameworks,[268] or Congress prioritizing the amount of budget authority provided to some core capabilities relative to others.[269]

National Health Security

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

According to the U.S. Department of Health and Human Services (HHS), "National health security is a state in which the nation and its people are prepared for, protected from, and resilient in the face of incidents with health consequences."[270] The nation's public health emergency management laws expanded considerably following the terrorist attacks in 2001 and Hurricane Katrina in 2005, in particular. Since then a varied slate of health incidents—including natural and man-made disasters and outbreaks of infectious disease—showed both improvements in the nation's readiness for public health and medical emergencies, and persistent gaps. For example, response plans may not sufficiently anticipate situations that arise. The technology needed to assess threats (such as radiation or chemical exposure) may be limited. Medical countermeasures (i.e., vaccines, antidotes, or treatments for harmful exposures) may not be available in adequate amounts, if at all. The means to distribute existing countermeasures in a timely manner may be limited. The medical system may lack adequate capacity to respond to mass casualty incidents. Funding for response costs may not be available immediately, or at all.[271] Given the robust roles of the private sector and state and local governments in health security efforts, the federal government's ability to address these gaps through funding assistance and other policies may also be limited.

Assistance under the Stafford Act can help federal, state, and local agencies with the costs of some types of public health emergency response activities, such as assuring food and water safety, and monitoring illnesses in affected communities.[272] However, there is no federal assistance program designed specifically to cover the uninsured or uncompensated costs of individual health care—including mental health care—that may be needed as a consequence of a disaster. There is no consensus that this should be a federal responsibility. Nonetheless, when confronted with mass casualty incidents, hospitals, physicians, and other health care providers may face considerable pressure to deliver care without a clear source of reimbursement. In addition, the response to a public health incident could necessitate activities that begin before Stafford Act reimbursement to HHS has been approved, or activities that are not eligible for Stafford Act reimbursement. Although the HHS Secretary has authority for a no-year Public

[268] For example, Congress may decide that one federal agency, such as HUD, 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 and the Recovery Federal Interagency Operational Plan.

[269] For 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." For basic descriptions of these and other core capabilities, see FEMA's website at https://www.fema.gov/core-capabilities.

[270] U.S. Department of Health and Human Services, "National Health Security Strategy and Implementation Plan—2015-2018," undated, p. 1, https://www.phe.gov/Preparedness/planning/authority/nhss/Pages/default.aspx.

[271] For further discussion see the National Health Security Preparedness Index, http://www.nhspi.org/.

[272] See CRS Insight IN10551, *Stafford Act Assistance for Public Health Incidents*; and FEMA Office of Response and Recovery, "Infectious Disease Event," Fact Sheet 104-009-001, May, 2006, https://www.fema.gov/media-library/assets/documents/99710.

Health Emergency Fund (PHEF), Congress has not appropriated monies to this fund for many years, and no funds are currently available.[273]

On several occasions Congress and the President have provided supplemental appropriations to address uncompensated disaster-related health care costs and unreimbursed state and local response costs flowing from a public health incident. These incidents include Hurricane Katrina,[274] the 2009 H1N1 influenza pandemic, the Haiti earthquake, Hurricane Sandy, and the Ebola and Zika virus outbreaks.[275]

Some policymakers, concerned about the inherent uncertainty in supplemental appropriations, have proposed dedicated funding approaches for public health emergency response. For FY2016, the Obama administration sought $110 million for the PHEF in its budget request.[276] Legislative proposals in the 114th Congress included H.R. 4525, which would have made a supplemental appropriation to the PHEF; S. 3280, which would have established a mechanism to appropriate and replenish funds to the PHEF; and H.R. 5926 and S. 3302, each of which would have established and provided appropriations to a contingency fund at the Centers for Disease Control and Prevention (CDC). None of these proposals were adopted.

Cybersecurity

Chris Jaikaran, Analyst in Cybersecurity Policy (cjaikaran@crs.loc.gov, 7-0750)

Cyberattacks pose a risk to the day-to-day processes of the U.S. economy and political system in a variety of ways, be it through disruption of economic activity, theft of intellectual property, compromise of critical infrastructure, espionage, or influence operations. Over the past decade, the United States has witnessed cyberattacks that have targeted both public sector and private sector data, sometimes stealing it, sometimes altering it, and sometimes denying access to it. The frequency of these attacks, and their potential effect on the economy, on our national security, and on people's lives has driven cybersecurity issues to the forefront of the national homeland security conversation. Development of sound cybersecurity policy at all levels of government and in the private sector represents a significant challenge for policymakers.

Given the technical nature of this issue and the impact of cybersecurity across the homeland security enterprise, this section of the report is less compartmentalized by sub-issue than other sections of this report. Instead, it seeks to lay a basis of understanding for the reader on the federal government's role in cybersecurity and begin to familiarize the reader with certain concepts currently in discussion, in order to facilitate understanding of the risks, challenges, and opportunities posed by information technology in the homeland security realm.

With that in mind, the section begins with a brief discussion about how cybersecurity may be defined, then examines how the federal government secures its networks and critical

[273] HHS, Assistant Secretary for Preparedness and Response, "Public Health Emergency Declaration Q&As," https://www.phe.gov/Preparedness/legal/Pages/phe-qa.aspx.

[274] GAO, *Hurricane Katrina: Allocation and Use of $2 Billion for Medicaid and Other Health Care Needs*, GAO-07-67, February 28, 2007, http://www.gao.gov/products/GAO-07-67.

[275] CRS Report R40531, *FY2009 Spring Supplemental Appropriations for Overseas Contingency Operations*; CRS Report R41232, *FY2010 Supplemental for Wars, Disaster Assistance, Haiti Relief, and Other Programs*; CRS Report R42869, *FY2013 Supplemental Funding for Disaster Relief*; CRS Report R43807, *FY2015 Funding to Counter Ebola and the Islamic State (IS)*; and CRS Report R44460, *Zika Response Funding: Request and Congressional Action*.

[276] HHS, "Public Health Emergency Response Initiative," Public Health and Social Services Emergency Fund, *Justification of Estimates for Appropriations Committees, FY2016*, p. 115, http://www.hhs.gov/budget.

infrastructure with the involvement of DHS. The next subsections examine the relationship of the public and private sector in providing cybersecurity, and how the federal government organizes its response to a "cyber incident" (like disaster response). A subsection discussing some specific technologies in the cybersecurity policy debate follows, and the section closes with some examples from the transportation security sector of how cybersecurity comes into play in ensuring stable operating environments.

Defining Cybersecurity

Chris Jaikaran, Analyst in Cybersecurity Policy (cjaikaran@crs.loc.gov, 7-0750)

The United States government does not have a single definition describing cybersecurity. However, the Commission on Enhancing National Cybersecurity's "Report on Securing and Growing the Digital Economy" offers the following:

> The process of protecting information and information systems by preventing, detecting, and responding to unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.[277]

The concepts of "confidentiality," "integrity," and "availability" are defined in U.S. Code as part of the "information security" triad. "Confidentiality" means that data is known only to authorized parties, "integrity" means that data is known to those parties in the manner they intend and not altered by another, and "availability" means that the data is available for access by those parties when they choose. These terms apply to the data stored, processed and transmitted by information technology (IT) systems, but also to the IT systems themselves. Growing in importance is a fourth term for information security—"authentication"—or the ability to confirm that parties using a system and accessing data are who they claim to be and have legitimate access to that data and system.

With the information security framework, cyberattacks can be categorized by what the attack compromises. For example, a data breach compromises confidentiality of information, malware that instructs a system to take an action the user did not authorize compromises integrity, and a denial of service attack compromises the availability of information.

Federal Network Security

Chris Jaikaran, Analyst in Cybersecurity Policy (cjaikaran@crs.loc.gov, 7-0750)

Compromise of federal government computer network security could cause significant disruption of day-to-day government functions, distort markets, economic activity, or threaten national security. The Federal Information Security Modernization Act (FISMA) establishes roles and responsibilities across the federal government for federal information technology security.[278] The Office of Management and Budget (OMB) is responsible for overseeing agency adoption of cybersecurity practices and requiring agencies have a cybersecurity posture commensurate to their risk. NIST develops mandatory standards (i.e., the Federal Information Processing Standards) and permissive guidance (i.e., Special Publications) on security practices agencies are to adopt. DHS oversees agency adoption of cybersecurity programs, provides tools to protect

[277] U.S. Commission on Enhancing National Cybersecurity, "Report on Security and Growing the Digital Economy," report, December 1, 2016, at https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf.

[278] 44 U.S.C. §3551.

agency networks, and coordinates government-wide efforts on federal cybersecurity. Inspectors General annually evaluate their agency's cybersecurity programs and provide recommendations on improving their cybersecurity posture.

Ultimately, however, the agency head is responsible for ensuring risks are effectively managed in their own agency. According to provisions in FISMA, the responsibility for cybersecurity shall be delegated to a senior official, frequently a chief information security officer.[279]

Federal agencies are much like industry when it comes to cybersecurity in that, for the most part, neither is developing custom hardware and software for its own use. Instead, the government, like critical infrastructure sectors, is usually reliant on third-party companies to develop and maintain the hardware and software employed at agencies.

The Congress exercises oversight over federal agency management, and the security of the agency's information technology is no exception. Congressional committees have held hearings on agencies' cybersecurity operations, frequently following a security incident. The appropriations committees and subcommittees consider an agency's cybersecurity efforts as they draft the annual appropriations bills.[280]

Information technology modernization has been growing as a topic for Congress to consider with regard to federal agency cybersecurity. GAO estimates that federal agencies spend over $80 billion annually on information technology.[281] In the 114th Congress, two bills in the House were merged and passed in the 114th Congress that would have granted agencies a dedicated working capital fund to finance technology modernization with the goal to spending less to secure and maintain older technology with inherent security vulnerabilities.[282]

Critical Infrastructure and Cybersecurity

Chris Jaikaran, Analyst in Cybersecurity Policy (cjaikaran@crs.loc.gov, 7-0750)

The national policy regarding critical infrastructure security and resilience seeks to achieve those conditions against all threats and all hazards. Cyber threats and hazards are considered major hindrances to security and resilience. As such, the government has invested in mitigating cybersecurity risks.

Critical infrastructure entities are under attack via cyberspace for a variety of reasons. Some attackers are seeking to steal trade secrets from targeted companies. Others are seeking information about the targets' customers or end users. There have been cyberattacks against critical infrastructure from nation-states, criminal organizations, and individuals, all of whom can pose a significant threat. Given the variety of motives and actors seeking to compromise critical infrastructure information and systems, owners and operators of critical infrastructure are encouraged by the government to adopt certain cybersecurity practices, and in some cases are required to do so by regulation. While not a national standard, the "Framework for Improving

[279] 44 U.S.C. §3554.

[280] For more information on federal spending on cybersecurity see CRS Report R44404, *Perspectives on Federal Cybersecurity Spending*, by William L. Painter and Chris Jaikaran.

[281] U.S. Government Accountability Office, *High Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others*, GAO-17-317, February 2017, p. 180, http://www.gao.gov/assets/690/682765.pdf.

[282] Elements of H.R. 4897 merged with H.R. 6004 in the 114th Congress before being passed in the House. There was not a companion bill in the Senate, nor was action taken on H.R. 6004 in the Senate before the Congress ended.

Critical Infrastructure Cybersecurity," more commonly known as the "NIST Cybersecurity Framework," provides entities with a structure and context to help manage their cyber risks.[283]

DHS serves as the lead federal agency for the delivery of resources to the private sector for cybersecurity and coordinating policy. In this capacity, the department encourages the sharing of information regarding cyber threats among companies and federal agencies. DHS facilitates the delivery of cyber threat analysis through its information sharing network, both analysis it has developed and the analysis of others. DHS offers tools to the private sector to help them understand their cyber risks and how to mitigate those risks as well as offering technical assistance (e.g., digital media analysis, investigations after a hack) when requested by a victim company.

Each critical infrastructure sector has a sector-specific agency (SSA) responsible for developing policy for and coordinating sector-specific security and resilience efforts with sector companies. Some agencies with an SSA role, such as the Department of Energy, have developed cybersecurity programs for the sectors for which they are responsible. Others, such as the Environmental Protection Agency, rely more on partnerships with other government agencies to inform their sector's cybersecurity posture.[284] The ability of an SSA to engage with its sector on cybersecurity is a function of the size (both in budget and manpower) of the agency, their primary responsibilities defined in law, and executive prioritization of agency activities.

Although the government offers assistance, it is ultimately the responsibility of the critical infrastructure owners and operators to consider their risk and put into effect policies and practices to mitigate that risk. Information technology vendors and industry associations assist CI owners and operators by providing goods and services tailored to the sector's needs.

Policy options exist to improve critical infrastructure cybersecurity. The NIST Cybersecurity Framework is currently in a review process to apply lessons learned from the past three years and to improve its applicability to adopters. Many cybersecurity experts encourage greater adoption of the Framework, but the question of whether it should be mandatory or a standard for industry to follow or face liability suits is still an open debate. To help critical infrastructure owners and operators improve their cybersecurity, incentives (e.g., grants, rate-recovery, and tax credits) have been considered but no proposal has been enacted or emerged as a favored approach.[285] Further regulation of cybersecurity among critical infrastructure sectors is an option, but some experts express concern that technology-specific cybersecurity regulations are counterproductive as the risk space changes faster than the regulations can adapt. Some of these experts prefer the concept of basing legislation and regulation on the desired effect instead.[286]

Government and Private Sector Roles in Cybersecurity

Chris Jaikaran, Analyst in Cybersecurity Policy (cjaikaran@crs.loc.gov, 7-0750)

[283] NIST, "Framework for Improving Critical Infrastructure Cybersecurity," report, February 12, 2014, at https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

[284] SSAs are assigned by national policy. For more information on SSAs and critical infrastructure security and resilience, see the National Infrastructure Protection Plan (NIPP) 2013 at https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf.

[285] For further information on cybersecurity incentives, see https://www.dhs.gov/sites/default/files/publications/dhs-eo13636-analytic-report-cybersecurity-incentives-study.pdf.

[286] CRS Video WVB00145, *Cybersecurity: How Can Congress Get Ahead of the Curve?*, by Eric A. Fischer.

As is the case with other aspects of homeland security, cybersecurity responsibilities are not solely vested in the federal government. Private firms, public utilities, other levels of government, and individuals all have impacts on the security of the global network and activities carried out on it.

The Obama Administration set forth a policy of cybersecurity as a shared responsibility. This approach asserts that there are roles for both the government and the private sector to play when it comes to ensuring our increasingly computing-reliant nation—whether government agencies, companies, or individuals—has proper cybersecurity strategies to choose from and adopt.[287] In outlining this shared responsibility, the policy envisioned different roles for each of these players.

Government could take direct action and regulate industry. On the other hand, government could convene industry with academia and government agencies to develop mutually acceptable and effective practices for various actors to implement. This latter course of action is frequently referred to as a public-private partnership. A third option is for the government to develop requirements—a set of characteristics it will mandate for products used by the government—which may then find their way into products for the private sector and general public.

Industry, for their part of the shared responsibility model, serves as the innovator. As a counterpoint to the government course of action, industry contributes to the marketplace and the national policy debate by offering new thinking, alternative concerns, varying viewpoints and novel research and development. As mentioned earlier, industry also provides the products (e.g., hardware, software, services) that all sectors of society use.

Cyber Response

Chris Jaikaran, Analyst in Cybersecurity Policy (cjaikaran@crs.loc.gov,7-0750)

In the wake of a cyber incident, like in the wake of a disaster, having an already-established plan for response and recovery can help minimize disruption and speed the return to normal activity.

The government has established a policy and general plan for how the government will respond to just such a cyber incident. Presidential Policy Directive 41 (PPD-41) outlines a few guiding principles for cyber response:

- response is a shared responsibility among the victims, the private sector, and the government;
- responses must be risked-based to determine which resources to bring to bear;
- any response must respect the affected entities, responses will require a unity-of-effort from across federal agencies; and
- any response should be done in a manner that enables restoration and recovery of operations to the victim, not just retaliation against the hacker.

PPD-41 also dictates that a government response will have concurrent lines of effort. “Threat response activities” will be led by the FBI and involve seeking out the hacker and delivering a response against them. “Asset response activities” will be led by DHS and involve efforts to help

[287] The White House, “Presidential Policy Directive—United States Cyber Incident Coordination,” presidential directive, July 26, 2016, at https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident.

victims mitigate the effects of an attack. The intelligence community will provide assistance to both lines of effort.[288]

Following the release PPD-41, the government adopted the National Cyber Incident Response Plan (NCRIP).[289] This plan follows a model as developed by the National Preparedness System under PPD-8, especially the National Response Framework, because it uses a core capability approach and adopts key aspects of the National Incident Management System (NIMS).[290] Instead of prescribing specific actions for agencies to take, the NCIRP outlines how the government will activate a Cyber Unified Coordination Group to address the specific incidents. This is similar to how the government, in response to a natural disaster, activates a multi-agency group at a Joint Field Office to deliver federal resources.

Lacking specific responses, or even a menu of options for the Cyber Unified Coordination Group to consider, the NCIRP is not an operational plan, and as such may not have a deterrent effect on adversaries.

Applied Technologies

Chris Jaikaran, Analyst in Cybersecurity Policy (cjaikaran@crs.loc.gov,7-0750)

Several technological developments represent challenges and opportunities in attempting to ensure "homeland cybersecurity." The following subsections explore encryption, automation, cloud computing, and the Internet of Things: four applications of technology with implications not only for our privacy and the efficiency of our economy, but also for our homeland security.

Encryption[291]

Encryption has been around for hundreds of years as a method to ensure the confidentiality of communications. In the information age, however, it is also being deployed as a means to ensure not only privacy of traditional communications, but also safeguarding intellectual property, financial transactions, and critical infrastructure—all of which are exposed to cyberspace in today's world. Understanding encryption's uses and limitations is an important part of understanding its potential impact on our homeland security.

Encryption is a process for transforming information into an unreadable form, which protects it from authorized access and manipulation. Encryption processes require five elements: the original information (the *plaintext*), which is an input to an *encryption method* and combined with a *key* to produce the *ciphertext.* To transform the encrypted information back to readable information, a *decryption method* is used with the ciphertext and the key to reproduce the original plaintext.

The application of encryption keeps data secure, but only in certain places. Data can be encrypted while it is stored, such as on a laptop or a phone, or while it is in transit, such as the email that is being sent. However, encryption cannot be applied to data while it is being created or edited—the document being filled out or the email being composed. So while encryption is a tool to ensure

[288] The White House, "Presidential Policy Directive—United States Cyber Incident Coordination," presidential directive, July 26, 2016, at https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident.

[289] Department of Homeland Security, "National Cyber Incident Response Plan," plan, December 2016, at https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf.

[290] For details on the National Response Framework, see https://www.fema.gov/national-response-framework.

[291] For more information see CRS Report R44642, *Encryption: Frequently Asked Questions*, by Chris Jaikaran.

confidentiality it cannot provide security at all times, especially on networks where data is regularly accessed, as that data is likely to remain in a state of being unencrypted to facilitate access and processing.

Systems using encryption as a way to ensure integrity can require a "signed command" before allowing that operation to run. A command can be cryptographically "signed" using encryption methods so the system can check to see if a command is legitimate. In this system, the command can execute if it can be verified using the systems encryption methods. Alternatively, if the file system is encrypted, any change to that system outside of the encryption method will cause an error in the system, alerting users to tampering.

Much has been written about encryption and the encryption debate during the 114th Congress. A large part of this debate was the "going dark" problem, of which encryption is one element.[292]

However, encryption also serves as a mitigating strategy from the risk posed by certain cyberattacks. As discussed earlier, there are a few elements to information security: confidentiality, availability, and integrity. There are many ways to attack availability such as denial of service attacks and ransomware attacks; there are also many ways to mitigate those attacks, such as increasing bandwidth and backups. However, there are fewer ways to mitigate than ways to attack. Encryption provides one of the few, effective ways to secure information against unwarranted access and to secure systems to ensure they operate in a trusted manner.

There are also ways to use encryption against users, such as with ransomware. Ransomware is a specific form of malware (malicious computer software) that installs itself on a user's computer and encrypts the user's hard drive so that the user cannot access their files. In this attack, the attacker has the key, so the victim's data is unreadable unless the attacker provides them the key to decrypt the data.

Automation

Automation has the potential to be disruptive to labor markets.[293] However, for homeland security, it also has the potential to improve cybersecurity. The government has a program that automates sharing of cyber threat indicators from machine to machine.[294] This is an example of machines taking autonomous action—in this case to facilitate information sharing and mitigation actions—without the influence from a human analyst. This has the potential to speed up the implementation of security practices, while also freeing up limited cybersecurity workforce resources to addressing areas of greater need.

Cloud Computing

Cloud computing is a computing model which enables constant, ubiquitous, on-demand access to shared computing resources (e.g., storage, appliances, computational power) over a network.[295] If

[292] The FBI defines the "going dark" problem as law enforcement having legal authority to intercept and access communications and information pursuant to court orders, but lacking the technical ability to carry out those orders because of a fundamental shift in communications services and technologies. For further information on "going dark," see CRS Report R44481, *Encryption and the "Going Dark" Debate*, by Kristin Finklea.

[293] The Executive Office of the President, "Artificial Intelligence, Automation, and the Economy," report, December 20, 2016, at https://obamawhitehouse.archives.gov/sites/whitehouse.gov/files/documents/Artificial-Intelligence-Automation-Economy.PDF.

[294] The Automated Indicator Sharing (AIS), http://dhs.gov/ais.

[295] NIST, "The NIST Definition of Cloud Computing," special publication 800-145, September 2011, at http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

one were running a business with a lack of cybersecurity workforce resources, migrating to a cloud architecture could free up company resources to be used on the company's main products or services. Cloud providers can offer dedicated security teams to ensure that the integrity and confidentiality of data remains secure.

However, cloud computing relies on a connection to the public Internet. Those who move their data to the cloud are then at the mercy of their cloud service host and their internet service provider. Enterprises that transition to a cloud provider could have difficulty accessing their data if their connection to the public Internet is disrupted or their cloud provider has a disruption in service.

Internet of Things

The Internet of Things (IOT) has already demonstrated that it poses a security concern.[296] IOT devices contain processing power, storage, and a network connection, and in many cases one or more sensors. This combination of features allows IOT devices to assist in the control of the physical world through the digital one. For instance, Internet-connected meters can report to utilities on power consumption, negating the need for meter-readers to physically visit each site. However, poorly secured devices pose a threat to other devices on the network and to the Internet as a whole by being the launch points for other attacks. Additionally, IOT devices may be the target of an attack, such as taking over a device to use it as a surveillance tool.

Policy options for potential legislation addressing aspects of evolving technologies may be difficult to consider, as governmental actions may lead to unintended consequences in the market for these emerging technologies—such as product lock-in (i.e., the establishing of a product as the accepted technology moving forward, at the detriment of competitors or competing technologies), raised costs, or reduced innovation. However, by not taking any action the government relegates policy decisions about these emerging technologies to the private sector companies building them, or forfeits leadership opportunities over the technologies to other countries willing to take action—and for which the policies developed by those countries may not align with American national or homeland security interests.

Cybersecurity in Selected Transportation Sectors

Aviation Cybersecurity

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

There is growing concern over cybersecurity threats to aircraft, air traffic control systems, and airports. TSA has indicated that its approach to cybersecurity thus far has not been through regulation, but rather through voluntary collaboration with industry. Under this framework, TSA formed the Transportation Systems Sector Cybersecurity Working Group, which created a cybersecurity strategy for the transportation sector in 2012.[297] Also, in coordination with the FBI and industry partners, TSA launched the Air Domain Intelligence Integration Center and an

[296] For further information on the Internet of Things, see CRS Insight IN10600, *Did a Thermostat Break the Internet?*, by Chris Jaikaran, and CRS Report R44227, *The Internet of Things: Frequently Asked Questions*, by Eric A. Fischer.

[297] Department of Homeland Security, "Executive Order 13636—Improving Critical Infrastructure Cybersecurity, Section 10(b) Report: TSA's Approach to Voluntary Industry Adoption of the NIST Cybersecurity Framework," http://www.dhs.gov/sites/default/files/publications/ExecutiveOrder_13636Sec10%28b%29Reportv5.pdf.

accompanying analysis center in 2014 to share information and conduct analysis of cyber threats to civil aviation.[298]

In recognition of cybersecurity threats, FAA has developed a software assurance policy for all FAA-owned and FAA-controlled information systems.[299] However, according to an April 2015 GAO report, while FAA has taken steps to protect air traffic control systems from cyber threats, it lacks a formal cybersecurity threat model. Moreover, GAO found that FAA faces continuing challenges in mitigating cyber threats, particularly as it transforms air traffic control systems under its NextGen modernization initiative.[300]

For systems onboard aircraft, FAA requires security and integrity to be addressed in the airworthiness certification process. Despite efforts to design aircraft systems to be resilient to cyber threats, in April 2015, TSA and the FBI issued warnings that the increasing interconnectedness of these systems makes them vulnerable to unauthorized access and advised airlines to look out for individuals trying to tap into aircraft electronics and for any evidence of tampering or network intrusions.[301]

Maritime Cybersecurity

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

In June 2015, the Coast Guard released a cyberstrategy document that identifies the agency's plans for addressing cybersecurity in the maritime environment. Vessel and facility operators use cyberdependent technologies for navigation, communication, cargo handling, and other purposes. The strategy document states the Coast Guard will be developing guidance for vessels and ports to address cybervulnerabilities, and will incorporate cybersecurity into existing enforcement and compliance programs.[302] The strategy also states the Coast Guard will incorporate cybersecurity training in the requirements for mariner licensing and for port security officer qualifications. According to this document, the Coast Guard will modify an existing port risk assessment tool (MSRAM-Maritime Security Risk Assessment Model) to incorporate cyber risks. MSRAM is the primary tool used to assess risk to national infrastructure in the maritime domain, and is used extensively at the local, regional, and national levels, according to the Coast Guard.

In the 114th Congress, House-passed H.R. 3878 sought to promote cybersecurity risk information sharing among maritime stakeholders and provide industry with risk assessment tools. House-passed H.R. 5077 required DHS to report on U.S. maritime cyber threats and vulnerabilities (sec. 604). The Senate did not act on either bill.

[298] Rachael King, "Aviation Industry and Government to Share Cyber Threats in New Intelligence Center," *Wall Street Journal CIO Journal*, April 15, 2014, http://blogs.wsj.com/cio/2014/04/15/aviation-industry-and-government-to-share-cyberthreats-in-new-intelligence-center/.

[299] Federal Aviation Administration, "Order 1370.109: National Policy, Software Assurance Policy," effective October 23, 2009.

[300] Government Accountability Office, *Air Traffic Control: FAA Needs a More Comprehensive Approach to Address Cybersecurity As Agency Transitions to NextGen*, GAO-15-370, April 2015.

[301] Kim Zetter, "Feds Warn Airlines to Look Out for Passengers Hacking Jets," *Wired*, April 21, 2015, http://www.wired.com/2015/04/fbi-tsa-warn-airlines-tampering-onboard-wifi/.

[302] U.S. Coast Guard, "Cyber Strategy," June 2015, pp. 32-33; https://www.uscg.mil/seniorleadership/DOCS/cyber.pdf.

DHS Management Issues

Unity of Effort

William L. Painter, Specialist in Homeland Security Policy and Appropriations
(wpainter@crs.loc.gov, 7-3335)

One of the unresolved debates from the development of DHS was 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 smaller management function that allowed components to function freely in their areas of expertise much as they had before.

Once the department was established, 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 strong leadership. 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 the department, 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 way of doing business by implementing new analytical and decisionmaking processes to develop strategy, plan, and identify joint requirements. 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 department, 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.[303]

The memorandum laid out four areas of initial focus. 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." The second area was to make improvements to the departmental management processes for investments. Specifically, incorporating strategic

[303] Secretary for Homeland Security Jeh Johnson, interviewed by Steve Watkins, "DHS Head: Cybersecurity, Unity of Effort Top Priority List," *Federal Times*, October 17, 2014. Available at http://www.federaltimes.com/article/20141017/DHS/310170024/.

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. The third was developing a stronger strategy, planning, and analytic capability within the Office of Policy. 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,[304] although there has been concern expressed about keeping Congress informed about progress and consequences of reorganizations in the field.[305]

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.

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.[306]

At the confirmation hearing for Gen. 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.[307]

Congress may debate the appropriate role of departmental level management at DHS, the level of engagement Congress should have as reforms go forward, the progress of management reforms, and whether they are having the desired effect.

Chemical, Biological, Radiological, Nuclear, and Explosives Office (CBRNE)

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

In 2013, Congress directed DHS to review its programs relating to chemical, biological, radiological, and nuclear threats and to evaluate "potential improvements in performance and possible savings in costs that might be gained by consolidation of current organizations and missions, including the option of merging functions of the Domestic Nuclear Detection Office (DNDO) and the Office of Health Affairs (OHA)."[308] The report of this review was completed in

[304] See H.Rept. 113-481, p. 7; S.Rept. 113-198, p. 16; H.Rept. 114-215, p. 4; H.Rept. 114-668, p. 5, and S.Rept. 114-264, p. 16.

[305] S.Rept. 114-68, p. 12.

[306] P.L. 114-328, Sec. 1901-1902.

[307] U.S. Congress, Senate Committee on Homeland Security and Governmental Affairs, *Nomination of General John F. Kelly, USMC (Ret.), to be Secretary, U.S. Department of Homeland Security*, 115th Cong., 1st sess., January 10, 2017. Official transcript is unavailable as of publication, but a Congressional Quarterly transcript can be found at http://www.cq.com/doc/congressionaltranscripts-5018456?4.

[308] Explanatory statement on the Consolidated and Further Continuing Appropriations Act, 2013 (P.L. 113-6), (continued...)

June 2015. In July 2015, DHS officials testified that DHS plans to consolidate DNDO, OHA, and smaller elements of several other DHS programs into a new office, led by a new Assistant Secretary, with responsibility for DHS-wide coordination of chemical, biological, radiological, nuclear, and explosives (CBRNE) "strategy, policy, situational awareness, threat and risk assessments, contingency planning, operational requirements, acquisition formulation and oversight, and preparedness."[309]

The FY2017 budget request reflected this proposed reorganization. The budget proposed establishing a Chemical, Biological, Radiological, Nuclear, and Explosives Office containing the Domestic Nuclear Detection Office (DNDO), the Office of Health Affairs (OHA), the CBRNE threat awareness and risk assessment activities of the Science and Technology Directorate, the CBRNE functions of the Office of Policy and the Office of Operations Coordination, and the Office of Bombing Prevention from the National Protection and Programs Directorate (NPPD). In the 114th Congress, the House passed H.R. 3875, which would have implemented this proposed restructuring. The Senate did not pass a similar bill.

Proponents of such a reorganization suggest that consolidating CBRNE activities would create a stronger focus within the department and improve interagency and interdepartmental coordination for these activities. However, skeptics of reorganization have questioned whether the benefits would outweigh the cost of disrupting current efforts, how well the differing agency cultures and missions would mesh, and why the new office would conduct research and development for nuclear defense but not biodefense.[310]

Common Appropriations Structure

William L. Painter, Specialist in Homeland Security Policy and Appropriations (wpainter@crs.loc.gov, 7-3335)

For further information, see CRS Report R44661, *DHS Appropriations FY2017: Departmental Management and Operations*.

When DHS was established in 2003, components of other agencies were brought together over a matter of months, in the midst of ongoing budget cycles. Rather than developing a new structure of appropriations for the entire department, Congress and the Administration continued to provide resources through existing account structures when possible.

In H.Rept. 113-481, accompanying the House version of the FY2015 Department of Homeland Security Appropriations Act, the House Appropriations Committee wrote: "In order to provide the Department and the Committees increased visibility, comparability, and information on which to base resource allocation decisions, particularly in the current fiscal climate, the Committee

(...continued)

Congressional Record, March 11, 2013, p. S1547.

[309] Joint prepared testimony of Reginald Brothers, Under Secretary for Science and Technology, Kathryn H. Brinsfield, Assistant Secretary for Health Affairs and Chief Medical Officer, and Huban A. Gowadia, Director of the Domestic Nuclear Detection Office, Department of Homeland Security, before the House Committee on Homeland Security, Subcommittees on Emergency Preparedness, Response, and Communications and Cybersecurity, Infrastructure Protection, and Security Technologies, July 14, 2015, http://homeland.house.gov/hearing/joint-subcommittee-hearing-weapons-mass-destruction-bolstering-dhs-combat-persistent-threats.

[310] Biodefense research and development would remain in the Science and Technology Directorate. See House Committee on Homeland Security, Subcommittees on Emergency Preparedness, Response, and Communications and Cybersecurity, Infrastructure Protection, and Security Technologies, July 14, 2015, http://homeland.house.gov/hearing/joint-subcommittee-hearing-weapons-mass-destruction-bolstering-dhs-combat-persistent-threats.

believes DHS would benefit from the implementation of a common appropriation structure across the Department." It went on to direct the DHS Office of the Chief Financial Officer "to work with the components, the Office of Management and Budget (OMB), and the Committee to develop a common appropriation structure for the President's fiscal year 2017 budget request."[311]

Section 563 of Division F of P.L. 114-113 (the FY2016 Department of Homeland Security Appropriations Act) provided authority for DHS to submit its FY2017 appropriations request under the new common appropriations structure (or CAS), and implement it in FY2017. Under the act, the new structure was to have four categories of appropriations:

- Operations and Support;
- Procurement, Construction and Improvement;
- Research and Development; and
- Federal Assistance.[312]

Most of the FY2017 DHS appropriations request categorized its appropriations in this fashion. The exception was the Coast Guard, which was in the process of migrating its financial information to a new system. DHS has also proposed realigning its Programs, Project, and Activities (PPA) structure—the next level of funding detail below the appropriation level—possibly trying to align PPAs into a mission-based hierarchy.

The Senate Appropriations Committee did not make its recommendation using the new structure, instead drafting its annual DHS appropriations bill and report using the same structure as was used in FY2016. The House Appropriations Committee made its recommendation using the new structure. Sec. 130 of the Continuing Appropriations Act, 2017 (P.L. 114-223) included specific authority for DHS to obligate resources provided under the continuing resolution in a revised CAS, and the Trump Administration's supplemental appropriations request for FY2017 indicated that the Administration was continuing to organize DHS funding on that basis.

Division F of P.L. 115-31 provided appropriations under a revised CAS for all DHS components except the U.S. Coast Guard, which has faced a series of challenges in updating its financial management systems. Congress will consider whether the new CAS provides the improved transparency it sought, whether the new PPA structure is sufficiently detailed, and also whether and how to integrate the Coast Guard into the new structures in the coming years.

DHS Headquarters Consolidation

William L. Painter, Specialist in Homeland Security Policy and Appropriations (wpainter@crs.loc.gov, 7-3335)

For additional information, see CRS Report R42753, *DHS Headquarters Consolidation Project: Issues for Congress*.

The Department of Homeland Security's headquarters footprint occupies more than 7 million square feet of office space in about 50 separate locations in the greater Washington, DC, area. This is largely a legacy of how the department was assembled in a short period of time from 22 separate federal agencies which were themselves spread across the National Capital region. The fragmentation of headquarters is cited by the department as a major contributor to inefficiencies,

[311] H.Rept. 113-481, p. 24.

[312] §563, Division F, P.L. 114-113.

including time lost shuttling staff between headquarters elements; additional security, real estate, and administrative costs; and reduced cohesion among the components that make up the department.

To unify the department's headquarters functions, the department approved a $3.4 billion master plan to create a new DHS headquarters on the grounds of St. Elizabeths in Anacostia. According to GSA, this is the largest federal office construction since the Pentagon was built during World War II. $1.4 billion of this project was to be funded through the DHS budget, and $2 billion through the GSA.[313] Thus far a total of over $2.5 billion has been appropriated for the project—$759 million for DHS and $1,548 million to GSA through FY2016. Phase 1A of the project—a new Coast Guard headquarters facility—has been completed with the funding already provided by Congress and is now in use.

In 2013, a revised construction schedule was developed, projecting lower levels of appropriations and a longer timeline for the project. Under the new projection, the project would be completed in FY2026 at a cost of $4.5 billion.[314] The project was criticized by GAO in September 2014 for not conforming to certain leading practices for capital decisionmaking processes. DHS and GSA revised its plans as a result of similar observations by GAO and other critics, announcing a new plan that would be completed in FY2021, and cost $3.7 billion.

According to GSA, even with the cost increases from delaying funding, the project would still result in over $430 million in projected savings compared to leasing over the next 30 years. This estimate does not take into account the costs GSA would have to incur to stabilize and maintain the St. Elizabeths campus if the project were halted, or the efficiencies for DHS that a consolidated headquarters would generate.[315]

With the Coast Guard now operating from St. Elizabeths, any discussions on headquarters consolidation in the 115th Congress are likely to focus on how to best use the available facilities on the campus, whether the latest revisions to the plan are acceptable to Congress, and how the headquarters consolidation will compete for resources within the DHS and GSA budgets.

Department of Homeland Security Personnel Issues

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

An essential consideration underlying the mission and performance of the Department of Homeland Security (DHS) is human resource management (HRM). Responsibility for HRM is vested in the Office of the Chief Human Capital Officer (OCHCO), an entity organizationally and for appropriations purposes located within the Under Secretary for Management. The OCHCO plays a critical role in supporting and executing the department's "Strategic Plan for Fiscal Years 2014-2018."[316] The Chief Human Capital Officer (CHCO) is the chief policy advisor on human resource management issues. At DHS, the CHCO is a career Senior Executive Service position. The incumbent CHCO assumed the position on January 11, 2016.

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

[314] "St. Elizabeths Development Revised Baseline," document provided by DHS, June 12, 2013.

[315] "Prospectus—Construction: Department of Homeland Security Consolidation at St. Elizabeths, Washington DC," PDC-0002-WA14, p. 14 as downloaded from GSA.gov.

[316] U.S. Department of Homeland Security, *Strategic Plan Fiscal Years 2014-2018* (Washington, DC: January 10, 2017), at https://www.dhs.gov/sites/default/files/publications/FY14-18%20Strategic%20Plan_0_0.PDF.

During the 115th Congress, the House of Representatives and the Senate may conduct oversight of personnel issues at DHS. Among the matters that may be considered are those related to the statutory responsibilities for the CHCO position, the department's human capital strategy for recruitment, millennials and federal government employment, the organizational culture at DHS, and collaboration between the department and its components through the Employee Engagement Steering Committee. Each of these issues is briefly discussed below. Hearings conducted by the House of Representatives and the Senate related to DHS appropriations or management matters could include review of these issues.

Each May, during Public Service Recognition Week, the value of public service is discussed and the work of public servants, including federal employees, is highlighted and honored. This observance[317] could provide an occasion for Congress to annually review human resource management at the department, either through meetings with DHS officials and the CHCO or an oversight hearing. Such activities could supplement congressional review and oversight of the OCHCO and current and developing HRM policies at DHS, throughout the year.

Chief Human Capital Officer (CHCO) Responsibilities

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

Title XIII, Sec. 1302 (The Chief Human Capital Officers Act of 2002) of P.L. 107-296, the Homeland Security Act of 2002, enacted on November 25, 2002, authorizes the position of CHCO in the Cabinet departments and selected independent agencies.[318]

The 114th Congress amended Section 704 of the Homeland Security Act to codify the responsibilities of the CHCO at DHS. Title XIX, Section 1904[319] of P.L. 114-328, the National Defense Authorization Act (NDAA) for Fiscal Year 2017 (S. 2943), enacted on December 23, 2016, specifies that the Chief Human Capital Officer reports directly to the Under Secretary for Management.[320] The law provides that the department's CHCO has 10 responsibilities[321] as follows:

[317] Public Service Recognition Week, at http://publicservicerecognitionweek.org/.

[318] The provision is codified at 116 Stat. 2135, at 2287; 5 U.S.C. Chapter 14. 5 U.S.C. §1402(a) provides that the functions of the CHCO include (1) setting the workforce development strategy of an agency; (2) assessing workforce characteristics and future needs based on an agency's mission and strategic plan; (3) aligning an agency's human resources policies and programs with organization mission, strategic goals, and performance outcomes; (4) developing and advocating a culture of continuous learning to attract and retain employees with superior abilities; (5) identifying best practices and benchmarking studies; and (6) applying methods for measuring intellectual capital and identifying links of that capital to organizational performance and growth.

[319] The law provides that nothing in this section overrides or otherwise affects the requirements of Section 888 of the Homeland Security Act of 2002 on preserving Coast Guard mission performance.

[320] The provisions on the DHS CHCO were added to the NDAA for FY2017 during the conference committee on S. 2943. They derive from a bill, S. 2976, the DHS Accountability Act of 2016, as reported (S.Rept. 114-287) by the Senate Committee on Homeland Security and Governmental Affairs on June 28, 2016. On May 23, 2016, Senator Ron Johnson introduced S. 2976. The Senate Committee marked up and ordered the bill to be reported as amended on May 25, 2016. During mark-up, the committee agreed to an amendment offered by Senator Heidi Heitkamp which added the provisions on the DHS CHCO to S. 2976. On December 27, 2016, DHS Secretary Jeh Johnson issued a statement on the passage of the NDAA for FY2017. See, U.S. Department of Homeland Security, Office of the Press Secretary, "Statement by Secretary Johnson on the Passage by Congress of the FY 2017 NDAA with Provisions for Strengthening the Department of Homeland Security," December 27, 2016, at https://www.dhs.gov/news/2016/12/27/statement-secretary-johnson-passage-congress-fy-2017-ndaa-provisions-strengthening.

[321] The law provides that these responsibilities are in addition to those stated in 5 U.S.C. Chapter 14 and other (continued...)

> (1) develop and implement strategic workforce planning policies that are consistent with Government-wide leading principles and in line with Department strategic human capital goals and priorities, taking into account the special requirements of members of the Armed Forces serving in the Coast Guard;
>
> (2) develop performance measures to provide a basis for monitoring and evaluating Department-wide strategic workforce planning efforts;
>
> (3) develop, improve, and implement policies, including compensation flexibilities available to Federal agencies where appropriate, to recruit, hire, train, and retain the workforce of the Department, in coordination with all components of the Department;
>
> (4) identify methods for managing and overseeing human capital programs and initiatives, in coordination with the head of each component of the Department;
>
> (5) develop a career path framework and create opportunities for leader development in coordination with all components of the Department;
>
> (6) lead the efforts of the Department for managing employee resources, including training and development opportunities, in coordination with each component of the Department;
>
> (7) work to ensure the Department is implementing human capital programs and initiatives and effectively educating each component of the Department about these programs and initiatives;
>
> (8) identify and eliminate unnecessary and duplicative human capital policies and guidance;
>
> (9) provide input concerning the hiring and performance of the Chief Human Capital Officer or comparable official in each component of the Department; and
>
> (10) ensure that all employees of the Department are informed of their rights and remedies under chapters 12 and 23 of title 5, United States Code.[322]

Under the law, each DHS component, in coordination with the department's CHCO, is directed to develop a five-year workforce strategy that will support DHS goals, objectives, and performance measures for determining the proper balance of federal employees and private labor resources.[323] In addition, the DHS Secretary is directed to submit a report related to workforce strategies and staffing to the House Committee on Homeland Security and the Senate Committee on Homeland Security and Governmental Affairs within 90 days after submitting the annual budget justification.[324]

(...continued)

applicable laws.

[322] 5 U.S.C. Chapter 12 covers the Merit Systems Protection Board, Office of Special Counsel, and Employee Right of Action. 5 U.S.C. Chapter 23 covers the Merit System Principles.

[323] Each component must consider the effect on human resources associated with creating additional federal full-time equivalent positions, converting private contractors to federal employees, or relying on the private sector for goods and services in developing the strategy.

[324] The report must include a table which shows actual and enacted amounts by component for each of the following: (1) information on the department's progress in fulfilling the workforce strategies; (2) the number of on-board federal employees from the prior fiscal year; (3) the total contract hours submitted by each prime contractor as part of the required service contract inventory; and (4) the number of full-time equivalent personnel identified under the Intergovernmental Personnel Act of 1970.

Congress may be interested in examining the fulfillment of the CHCO's statutory responsibilities, including the policies and programs that are established, implemented, and evaluated to carry them out. Congress could also review the department's workforce strategies and staffing plans.

Human Capital Strategy for Recruitment

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

The responsibilities of the CHCO at DHS are centered around human capital planning. According to the Office of Personnel Management (OPM):

> human capital planning is the method by which an agency designs a coherent framework of human capital policies, programs, and practices to achieve a shared vision integrated with the agency's strategic plan. Implementation of the strategic human capital plan is a key step in an agency's progress to build a highly effective, performance-based organization by recruiting, acquiring, motivating, and rewarding a high-performing, top quality workforce. The plan becomes the road map for continuous improvement and the framework for transforming the culture and operations of the agency.[325]

An agency's recruitment strategy is part of its human capital strategic plan. DHS's planning process for hiring new employees is reportedly underway.[326] Recruitment will occur against the backdrop of a recently-expired government-wide hiring freeze and directives to hire a specified number of employees in U.S. Immigration and Customs Enforcement (ICE) and U.S. Customs and Border Patrol (CPB). A Presidential Memorandum issued by President Donald Trump on January 23, 2017, instituted a 90-day hiring freeze in executive agencies.[327] Executive Orders issued by President Trump on January 25, 2017, directed CBP to hire 5,000 border patrol officers and ICE to hire 10,000 Immigration Officers, subject to available appropriations, respectively.[328]

In testimony provided to the Senate Committee on Homeland Security and Governmental Affairs, Subcommittee on Regulatory Affairs and Federal Management in September 2016, the department's CHCO, Angela Bailey, stated that a "DHS Strategic Outreach and Recruitment

[325] U.S. Office of Personnel Management, "Key Components of a Strategic Human Capital Plan," September 2005, at https://www.opm.gov/policy-data-oversight/human-capital-management/reference-materials/strategic-alignment/keycomponents.pdf. OPM regulations codified at 5 C.F.R. §250.203 establish requirements for an agency to maintain a current human capital plan and submit to OPM an annual human capital accountability report. OPM is the central personnel management agency for the executive branch.

[326] In 2016, that process reportedly included hiring through events that were conducted in person or by using online platforms. The department hosted an in-person job fair in July 2016, for cyber and tech positions. A virtual hiring fair occurred in December 2016, for positions across the department. Nicole Ogrysko, "2 Big Hiring Events Inform DHS' Recruitment Strategy in 2017," Federalnewsradio.com, January 27, 2017, at http://federalnewsradio.com/hiringretention/2017/01/two-big-hiring-events-inform-dhs-recruitment-strategy-2017/.

[327] U.S. President (Trump), Memorandum of January 23, 2017, "Hiring Freeze," *Federal Register*, vol. 82, January 25, 2017, pp. 8493-8494, at https://www.gpo.gov/fdsys/pkg/FR-2017-01-25/pdf/2017-01842.pdf. Office of Personnel Management (OPM) and Office of Management and Budget (OMB) guidance to implement the hiring freeze are included in Memorandum to Heads of Executive Departments and Agencies, M-17-18, from Mark Sandy, Acting Director, OMB, and Kathleen McGettigan, Acting Director, OPM, "Federal Civilian Hiring Freeze Guidance," January 31, 2017, at https://www.chcoc.gov/content/federal-civilian-hiring-freeze-guidance. An internal DHS document identifies positions in the department and its components which have been exempted from the freeze.

[328] U.S. President (Trump), Executive Order 13767 of January 25, 2017, "Border Security and Immigration Enforcement Improvements" (Sec. 8), *Federal Register*, vol. 82, January 30, 2017, pp. 8793-8797, at https://www.gpo.gov/fdsys/pkg/FR-2017-01-30/pdf/2017-02095.pdf. U.S. President (Trump), Executive Order 13768 of January 25, 2017, "Enhancing Public Safety in the Interior of the United States" (Sec. 7), *Federal Register*, vol. 82, January 30, 2017, pp. 8799-8803, at https://www.gpo.gov/fdsys/pkg/FR-2017-01-30/pdf/2017-02102.pdf.

(SOAR) Plan" had been prepared and is "focused on recruiting a highly qualified and diverse workforce."[329] The testimony identified several of the department's mission critical occupations, including Transportation Security Administration (TSA) officers; CBP officers; Emergency Management personnel at the Federal Emergency Management Agency (FEMA); Budget, Cost, Internal Control, and Resource Analysts; and Accountants.[330]

Congress may be interested in examining the implementation and impacts of the hiring freeze and follow-on hiring policies on DHS, including positions exempted from hiring restrictions; the implementation of the Executive Order directives on hiring at ICE and CBP; and the department's recruitment strategy, especially as it relates to mission-critical occupations. Congress could also consider directing the department to include links to the relevant HRM policy documents on the OCHCO webpage to facilitate oversight.[331]

Millennials and Federal Government Employment

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

Millennials[332] who are considering employment with the federal government may be especially interested in the DHS recruitment strategy. Congress conducted oversight on the issue of millennials and federal employment in 2016. The Senate Committee on Homeland Security and Governmental Affairs, Subcommittee on Regulatory Affairs and Federal Management, for example, conducted a hearing titled *Understanding the Millennial Perspective in Deciding to Pursue and Remain in Federal Employment* on September 29, 2016. The Subcommittee Chairman, Senator James Lankford, and the Ranking Member, Senator Heidi Heitkamp, noted the retirement eligibility of a significant portion of the federal workforce over the next several years and the importance of recruiting and retaining "a new generation of federal employees."[333] In his opening statement, Senator Lankford cited "the fact that many millennials believe government service is not a rewarding or fulfilling job" as an obstacle in hiring.[334] Senator Heitkamp's opening statement expressed her belief that "it is important for the federal government to connect with the millennial generation in a way that speaks to their needs and their desire to pursue mission-oriented careers, while also demonstrating all that a career in the federal government has to offer."[335]

---

[329] U.S. Congress, Senate Committee on Homeland Security and Governmental Affairs, Subcommittee on Regulatory Affairs and Federal Management, Hearing, "Understanding the Millennial Perspective in Deciding to Pursue and Remain in Federal Employment," 114th Cong., 2nd sess. (Washington: GPO, September 29, 2016), p. 50, at https://www.gpo.gov/fdsys/pkg/CHRG-114shrg23786/pdf/CHRG-114shrg23786.pdf. Hereafter referred to as "Understanding the Millennial Perspective." A literature search did not reveal a publicly available copy of the SOAR plan. The search revealed references to, but not a publicly available copy of, a strategic human capital plan for the department as a whole. A DHS component, the Federal Emergency Management Agency (FEMA), posts its plan, "FEMA Human Capital Strategic Plan Fiscal Years 2016-2020," at https://www.fema.gov/media-library-data/1465232797001-0884912c49ec300ced75c391a0dc81dc/HumanCap_Final_Version.pdf.

[330] Ibid., pp. 51-52. A literature search did not reveal a publicly available copy of a comprehensive list of the department's mission-critical occupations.

[331] https://www.dhs.gov/organization/ochco-office-chief-human-capital-officer.

[332] Millennials are defined by the Senate Committee on Homeland Security and Governmental Affairs as individuals born after 1980 and currently under age 35.

[333] "Understanding the Millennial Perspective," p. 1.

[334] Ibid.

[335] Ibid., p. 41.

Stating that, "millennials are identified as a key demographic in our recruitment strategy," Angela Bailey, CHCO at DHS, provided testimony to the committee that

- millennials represent approximately 21% of the DHS workforce, compared to 18.68% across the federal government;
- over 50% of millennials at DHS identify as a member of a diverse racial or ethnic group; and
- some 36% of millennials at DHS are women.[336]

She also stated that younger millennials under age 30 represent approximately 9% of the DHS workforce (compared to 7% across the federal government); 59% identify as a member of a diverse racial or ethnic group; and 42% are women. According to the CHCO, millennials are employed in mission-critical occupations across the department, and include more than 17,000 Transportation Security Officers at TSA, almost 11,000 CBP officers and Border Patrol Agents, and almost 300 Emergency Management personnel at FEMA.[337]

During an interview with a federal news organization in early July 2016, the CHCO said, with regard to recruitment:

> It is okay to have this in-and-out of government career. We are really okay with the fact that in some ways, you become an ambassador for us. If we at least create the best experience that we can, that you gain the most knowledge that can from this, and that you then take it to your private sector career.... We're not looking for 30-year-career employees. We're actually looking for folks that want to come in, they want to get this excellent experience and then they take it to the private sector, and then they come back again.[338]

DHS Excellence in Leadership (DEL) is an official, independent employee association at the department. The organization's mission is "to foster 'Unity of Effort' through professional development and community engagement."[339] The organization's webpage posts information on issues of interest to members, including federal employment of millennials.[340]

Congress may be interested in examining HRM policies and programs for millennials, including the recruitment strategy, recruitment and retention rates, and demographics for this workforce

[336] Ibid., pp. 50, 51.

[337] Ibid., p. 51.

[338] Nicole Ogrysko, "DHS: We're Not Looking for the 30-Year Career Employee," Federalnewsradio.com, July 5, 2016, at http://federalnewsradio.com/hiringretention/2016/07/dhs-not-looking-30-year-career-employee/. The article also quoted the CHCO's view: "With more flexibility to move in and out of government, Bailey also envisions a scenario where she can offer a pay and benefits package based on the project the department hires the employee for and the person's individual needs—rather than the traditional defined benefits package most federal employees under the General Schedule now have." (The General Schedule is the pay system for federal civilian white-collar employees whose jobs are described by position classification.)

[339] According to the organization's website, DHS Excellence in Leadership was chartered in July 2011 by a group of DHS employees formerly known as Homeland Young Professionals (HYP). HYP evolved into DHS Emerging Leaders and eventually DHS Excellence in Leadership, in order to be more inclusive of all leaders within the DHS community. DEL's current membership consists of over 500 employees across all components and divisions (https://dhsemergingleaders.wordpress.com/about/).

[340] "An Insight on the Thoughts of Millennials in Federal Government," November 7, 2016, at https://dhsemergingleaders.wordpress.com/2016/11/07/an-insight-on-the-thoughts-of-millennials-in-federal-government/. The article discusses the results of a survey conducted by federalnewsradio.com titled, "The Millennial Perspective in the Federal Government," that were reported in late June 2016, at http://1yxsm73j7aop3quc9y5ifaw3.wpengine.netdna-cdn.com/wp-content/uploads/2016/06/Millennial-Survey.pdf.

within the department and its components. Congress could also encourage the department to survey its millennial employees with regard to their experiences in working for DHS, perhaps in coordination with DHS Excellence in Leadership.

Organizational Culture at DHS

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

In June 2006, then-DHS Secretary Michael Chertoff "directed the Homeland Security Advisory Council (HSAC) to establish a Culture Task Force (CTF) to provide recommendations for creating, achieving and maintaining an empowering, energetic, dedicated, mission-focused culture within the Department and within the spectrum of its state, tribal, local and private sector partners." The Task Force report, issued on January 23, 2007, included recommendations that it believed would assist the Secretary and DHS leaders in creating and sustaining an organization "that leverages, focuses, strengthens and synergizes the multiple capabilities of its components and empowers them to continuously improve the Department's operational capacities and the security of the Nation."[341]

According to the report, "'Culture' is about people relationships and inspirations, and how the people of the Department view its Leadership, the organization itself and its purposes, and the importance of one's individual role within the Department."[342] Among the report's six recommendations were suggestions that the department (1) implement homeland security management and leadership models and (2) create leadership-empowered teamwork and a "Blended Culture." In making the first recommendation, the task force found that DHS should adopt two models: "a closed loop management model that sets the key relationships between strategic accountabilities, organizational units, performance expectations and management processes to achieve DHS goals" and "a leadership and training model, including 'joint duty and training' experience that will help all DHS leadership to focus collaboratively on key leadership expectations and objectives."[343] With regard to the second recommendation, the task force found that "No single Homeland Security culture is possible or—for that matter—wise. DHS must leverage its Components' unique cultures to create organizational and operational capacities greater than is the sum of their parts."[344]

On September 19, 2016, then-DHS Secretary Jeh Johnson and then Deputy Homeland Security Secretary Alejandro Mayorkas issued a fact sheet titled, "Changing the Culture at DHS." The document stated that the DHS officials "have made employee engagement and morale one of their highest priorities and have taken action to create an engagement-supportive culture across DHS." The document affirmed policies and listed action steps in five areas related to departmental management: (1) active involvement of a strong Employee Engagement Steering Committee (EESC); (2) recognizing and rewarding excellence in pursuit of mission; (3) enhancing communication; (4) increasing leadership accountability, awareness, and

[341] U.S. Homeland Security Advisory Council, "Report of the Culture Task Force," January 2007, pp. 1, 9, at https://www.dhs.gov/xlibrary/assets/hsac-culture-010107.pdf.

[342] Ibid., p. 7.

[343] Ibid., p. 3.

[344] Ibid., p. 5.

empowerment related to employee engagement; and (5) increasing transparency and fairness in the hiring and promotion process.[345]

Congress may be interested in reviewing the department's initiatives related to organizational culture, employee engagement, and the implementation and results of the Culture Task Force Report recommendations and the fact sheet on changing the culture of DHS. Congress could also examine coordination between the department's strategies related to organizational culture and the "Unity of Effort" initiative[346] and DHS implementation of any policies on joint duty assignments for employee development.

Interagency Collaboration through Employee Engagement Steering Committee

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

In December 2016, the Homeland Security and Defense Business Council and its member company, Grant Thornton, released the second survey of its five-year 20/20 Project on the Homeland Security Enterprise (HSE). According to the document, "The overall Project aims to capture perspectives from government and industry executives engaged in homeland security missions on critical challenges and future opportunities facing [DHS] and the broader interagency and public-private partnership that is the [HSE]." The survey identified interagency collaboration as an example of an excellent management practice that "exist[s] across DHS that should be acknowledged, examined, and replicated."[347]

Within the department, the EESC has a central role in coordinating interagency collaboration among DHS components that work together "on common DHS-wide programs" and implement "customized initiatives reflecting their particular needs and cultures." The Under Secretary for Management chairs the committee, which is made up of leaders from the department's operational components. The leaders are to "advise DHS leadership on their perspectives for department-wide approaches," share "best practices and brainstorming ideas" and report "on what is working and what needs to be improved."[348]

During an April 27, 2016, hearing conducted by the House Committee on Oversight and Government Reform, Subcommittee on Government Operations, the DHS CHCO, Angela Bailey, provided testimony that the steering committee's input had informed a new employee action engagement plan applicable department-wide. She said that the action plan focuses on "selecting and empowering high performing leaders, developing excellent leaders at all levels, and enhancing communication."[349] With regard to the communication focus, a DHS report explained

[345] U.S. Department of Homeland Security, "Fact Sheet: Changing the Culture at DHS," September 19, 2016, at https://www.dhs.gov/news/2016/09/19/fact-sheet-changing-culture-dhs. Hereinafter referred to as Changing the Culture at DHS Fact Sheet. According to the DHS CHCO, employee engagement at the department increased from 53% in 2015 to 56% in 2016 ("Understanding the Millennial Perspective," p. 54).

[346] The "Unity of Effort" initiative has been underway in the department since April 2014. The initiative involves efforts to conduct DHS operations in a more unified way and to develop a culture within the department that is supportive of this approach. See U.S. Department of Homeland Security, Memorandum for DHS Leadership, from Secretary Johnson, April 22, 2014, at http://www.hlswatch.com/wp-content/uploads/2014/04/DHSUnityOfEffort.pdf.

[347] Homeland Security Defense Business Council and Grant Thornton, The Homeland Security and Defense Business Council 20/20 Project on the Homeland Security Enterprise, *Charting the Future: A Mission Driven Homeland Security Enterprise*, December 2016, p. 3, at https://homelandcouncil.org/2020projectreport2016.pdf. Data collection for the survey occurred from September 2016 through November 2016. The survey methodology is stated on p. 1.

[348] Changing the Culture at DHS Fact Sheet.

[349] U.S. Congress, House Committee on Oversight and Government Reform, Subcommittee on Government (continued...)

that this referred to "two-way communication and inclusion utilizing labor management forums, diversity and inclusion councils, and ideation platforms."[350]

Congress may be interested in examining the department's existing policies and planned initiatives related to collaboration between DHS and its components and the operation and activities of the EESC. Congress could also direct the department to publish a link to the employee engagement action plan, and any other related HRM policy documents, on the OCHCO's webpage.

Author Contact Information

William L. Painter
Specialist in Homeland Security and Appropriations
wpainter@crs.loc.gov, 7-3335

(...continued)

Operations, Hearing, "The Best and Worst Places to Work in the Federal Government," 114th Cong., 2nd sess. (Washington: GPO, April 27, 2016), pp. 17-18, at https://www.gpo.gov/fdsys/pkg/CHRG-114hhrg20557/pdf/CHRG-114hhrg20557.pdf. A literature search did not reveal a publicly available copy of the employee action engagement plan.

[350] U.S. Department of Homeland Security, "Management Directive 715, Equal Employment Opportunity Program Status Report, Fiscal Year 2015" (Washington: DHS, [June 16, 2016]), p. 6, at https://www.dhs.gov/sites/default/files/publications/fy-2015-md-715-report.pdf.