Ten years later

Major Homeland Security Mandates of the 9/11 Commission Act

U.S. House of Representatives
Committee on Homeland Security
Rep. Bennie G. Thompson, Ranking Member

Minority Staff Report

THIS PAGE INTENTIONALLY LEFT BLANK

TEN YEARS LATER: MAJOR HOMELAND SECURITY MANDATES OF THE 9/11 COMMISSION ACT

To mark the tenth anniversary of the *Implementing Recommendations of the 9/11 Commission Act of 2007*, Committee on Homeland Security Ranking Member Bennie G. Thompson directed staff to review the Department of Homeland Security's progress with respect to ten of the most prominent mandates in the Act and, as appropriate, issue recommendations.

EXECUTIVE SUMMARY

INTRODUCTION

September 11, 2017 marks the sixteenth anniversary of the deadliest terrorist attack on U.S. soil. On that devastating day, 19 terrorist hijackers seized four passenger aircraft and purposely crashed them into iconic buildings—the Twin Towers and Pentagon—and, due to the heroism of passengers who overtook the cockpit, a Pennsylvania field. The 9/11 attacks resulted in the deaths of thousands of Americans, inflicted billions of dollars of economic damage, and instilled shock and fear throughout the homeland. In the wake of the attacks, Americans sought answers and efforts were redoubled to make the Nation more secure.

In November 2002, Congress took two major steps to bolster the security of the Nation. First, Congress enacted legislation to merge 22 existing Federal agencies into the Department of Homeland Security (DHS or the Department) to focus on preventing terrorist attacks, strengthening the homeland security enterprise (HSE), and enhancing the Nation's preparedness, response, and resilience to homeland security threats. Second, Congress established the bipartisan National Commission on the Terrorist Attacks Against the United States (9/11 Commission or the Commission) to investigate the attacks.

In 2004, the Commission released its final report which set out, in great detail, how al Qaeda plotted, trained, and carried out the attacks. It also provided dozens of critical recommendations for Federal action. Many of the most critical and difficult recommendations went unaddressed until the enactment, in 2007, of the *Implementing Recommendations of the 9/11 Commission Act of 2007* (P.L. 110-53) (the *9/11 Commission Act).*

In the ten years since the enactment of the *9/11 Commission Act*, the terrorist threat landscape has evolved. It has diversified and splintered to encompass numerous al Qaeda affiliates—most notably Al Qaeda in the Arabian Peninsula (AQAP)—as well as the Islamic State of Iraq and the Levant (ISIL). In April 2017, then-Secretary of Homeland Security John F. Kelly warned that the terrorist "threat has metastasized and decentralized, and the risk is as threatening today as it was that September morning almost 16 years ago." A few months later, Secretary Kelly assessed the potential for self-directed "lone wolf" attacks as about the same in "New York City, the largest municipality in the country, or in some little town in the middle of Arkansas." Since the 9/11 attacks, the nature of incidents has shifted away from complex, coordinated operations carried out by trained and funded operatives against high profile targets, to attacks carried out by individuals with little to no training or support, such

as active shooter attacks, homemade improvised explosive devices, and vehicular manslaughter.

Today, America is far better equipped than it was on September 11, 2001, to prepare for, prevent, and respond to acts of terrorism and other catastrophic events. The gains in preparedness are exemplified by the heroic responses to the Boston Marathon Bombings in 2013, the San Bernardino terrorist attack in December 2015, the Orlando night club mass shooting in June 2016, and the New York/New Jersey bombings in October 2016. Since 9/11, Federal investments in local preparedness and bolstering information sharing have helped deliver measurable progress in the level of security across the Nation. Still, we must stay vigilant and fully-engaged with homeland security partners to effectively address the dynamic range of threats that, in addition to traditional terrorist threats, today include cybersecurity attacks on critical infrastructure and violence by neo-Nazi, white supremacist, anti-government, and other domestic terror groups.

TEN MAJOR DHS MANDATES: THE STATE OF PLAY

I. Homeland Security Grants *(Sec. 101)*

On September 11, 2001, first responders heroically ran into unknown dangers to save as many lives as possible. However, their efforts were undermined by a national failure to adequately invest in building and maintaining a robust emergency management and response infrastructure and a coordinated communications system. Enactment of the *9/11 Commission Act* triggered substantial investments in first responder capabilities, with funding for the State Homeland Security Grant Program (SHSGP) and Urban Area Security Initiative (UASI) peaking at $950 million and $868 million, respectively. The response to the April 2013 Boston Marathon Bombings demonstrated how, with Federal support, first responder capabilities have improved since the 9/11 attacks. Unfortunately, in recent years, the arbitrary discretionary spending caps imposed by the *Budget Control Act of 2011* have significantly curtailed DHS' efforts to support critical State and local homeland security preparedness and response.

Congress and the Administration should take a range of actions including restoring needed funding, improving the grant risk formula, providing support to former UASI cities that, because of budget constraints, were eliminated from the program, authorizing the Nonprofit Security Grant Program, and helping enhance cybersecurity capabilities at the State and local levels.

II. Interoperability *(Sec 301)*

Emergency communications failures during the 9/11 attacks costed lives. The communications systems of emergency response agencies were overwhelmed by the amount of users, suffered from weak radio signal strength, and were not interoperable across jurisdictions and across disciplines. The *9/11 Commission Act* directed the Department to address these interoperability challenges at the State level by creating a targeted interoperability grant program and conditioning grant funding on compliance with governance plans. Between Fiscal Year (FY) 08 through FY11, Congress appropriated $50 million annually in interoperability grant funding, but under the Republican-controlled Congress, funding for the program was eliminated in FY12.

To ensure the continuation of critical interoperability efforts, particularly governance efforts, Congress should provide new resources. Additionally, Congress should act to ensure that major jurisdictions that rely upon the T-Band radio spectrum for mission critical voice capabilities—Boston, Chicago, Dallas, Houston, Los Angeles, Miami, New York, Philadelphia, Pittsburgh, San Francisco, and Washington, DC—continue to have access to it until capabilities are available on the Public Safety Broadband Network.

III. Information Sharing *(Secs. 501 and 511)*

The inability of Federal government and State, local, tribal and territorial (SLTT) partners to effectively disseminate information regarding terrorist threats represented a critical failure during the 9/11 attacks. Since that time, information sharing regarding terrorism threats has improved due to implementation of the *9/11 Commission Act*. Today, there are numerous channels for the sharing of threat information; these channels include National Terrorism Advisory System (NTAS) bulletins that disseminate timely threat information to the public via a web-based platform (the Homeland Security Information Network (HSIN)), where Sensitive But Unclassified Information is accessed by appropriate SLTT officials. Over the past decade, DHS has prioritized helping SLTT participate in fusion centers by making available Secret-level terrorism-related information to analysts and sponsoring security clearances for SLTT personnel.

DHS should continue to support fusion centers, work to remove obstacles that hinder the timely sharing of terrorist threat information, and continue to refine its channels for sharing threat information to ensure that they evolve to address the threat landscape and SLTT stakeholder needs.

IV. Modernization of the Visa Waiver Program/Biometric Entry-Exit System (*Sec. 711)*

Under the Visa Waiver Program (VWP), foreign nationals from 38 countries are eligible to visit the United States without obtaining a visa. The *9/11 Commission Act* required DHS to establish a biometric exit system by August 3, 2008, to record the departure of VWP visitors traveling by air, and an electronic travel authorization system through which foreign nationals electronically provide, in advance of travel, biographical information to determine VWP eligibility. On January 12, 2009, DHS announced full implementation of an electronic travel authorization program, the Electronic System for Travel Authorization (ESTA) for all VWP visitors traveling to the U.S. by airplane or cruise ship. DHS continues to strive towards implementing a biometric exit system but has encountered a variety of challenges. In 2016, then-DHS Secretary Jeh Johnson committed to implementing a biometric exit system at airports by 2018 and in early 2017, President Trump issued an Executive Order that called for such a system to be implemented.

To ensure that DHS can effectively implement the biometric exit system within its timeframe, it will have to take the following actions: immediately prioritize U.S. Customs and Border Protection Officer (CBPO) staffing at airports and other ports of entry, actively engage with the privacy community to ensure compliance with the Privacy Act, and consider establishing an advisory committee with private sector stakeholders.

V. Air Cargo Security *(Sec. 1602)*

The 9/11 Commission Report expressed concerns about screening and transport of checked bags and cargo and, in particular, "the threat posed by explosives in vessels' cargo holds." The *9/11 Commission Act* required DHS to establish a system to screen 100 percent of cargo transported on passenger aircraft, within three years after the date of enactment. On August 2, 2010, DHS announced the deadline was met for domestic passenger flights through the implementation of the Certified Cargo Screening Program (CCSP). While CCSP has improved air cargo security, more must be done to enhance air cargo security in light of continued terrorist interest in carrying out such attacks, as evidenced by the report, in late August, that Australian authorities foiled an air cargo-based attack.

The Transportation Security Administration (TSA) should review its air cargo security policies and regulations and make necessary updates to reflect changes in cargo volume and threats to the sector, centralize air cargo security responsibilities into one office, and evaluate whether third-party canine teams can be utilized to augment cargo screening operations. DHS, for its part, should make the Air Cargo Advance Screening (ACAS) program permanent to bolster supply chain security.

VI. Surface Transportation Grants and Training *(Secs. 1406, 1408, 1517, and 1534)*

Given the aviation sector's heightened security after the 9/11 attacks, terrorists view public surface transportation—such as freight and passenger trains, metros, subways, buses, and ferries—as soft targets for mass-casualty attacks. The lethality of mass transit attacks is far higher than other terrorist attacks, with an average of 16.3 people killed per device, which is 12.5 times more than those killed in other attacks. In order to bolster security, the *9/11 Commission Act* authorized the Transit Security Grant Program (TSGP) to provide dedicated funding to the Nation's mass transit systems. The program's funding peak came in FY08, when it was funded at nearly $389 million; however, funding plummeted to just $88 million in FY17, leaving jurisdictions without adequate resources. The Act also directed DHS to require baseline security training for frontline workers in public transportation within a year of enactment. On December 16, 2016, TSA published a proposed rule for baseline security training that received 30 comments from a diverse range of surface transportation stakeholders.

Looking ahead, TSA should act expeditiously to finalize training regulations in a manner that is responsive to stakeholder comments, and engage with stakeholders about opportunities for advanced training and exercises. Congress, for its part, should provide at least $200 million in TSGP funding.

VII. Maritime Cargo Security *(Sec. 1701)*

In 2003, a report commissioned by the U.S. Department of Transportation estimated that the economic impact of a nuclear terrorist attack on a major U.S. seaport "would create disruption of U.S. trade valued at $100-200 billion, property damage of $50-500 billion, and 50,000 to 1,000,000 lives. . . lost." In 2006, Congress enacted a law to require DHS to work with Federal and international partners to ensure that all U.S.-bound containers were scanned "as soon as possible" through an integrated non-intrusive inspection (NII) and radiation detection system before arriving in the U.S. The *9/11 Commission Act* amended that law to require that, no later than July 1, 2012, DHS complete full-scale implementation of the integrated scanning system and prohibit any U.S.-bound container from entering a U.S.-port unless it had been scanned at a foreign port. In recognition of the challenges associated with implementing this mandate, the law permitted DHS to extend the deadline for two years at one or more ports, if the DHS Secretary certifies that certain conditions exist. Since 2012, DHS has extended the deadline three times without specifying what obstacles were encountered in each port. The latest extension is set to expire in July 2018. On May 2, 2016, DHS published a Request for Information (RFI) soliciting "strategies to improve maritime supply chain security and achieve 100% overseas scanning." According to DHS, nearly all arriving cargo goes through radiation portal monitors at a U.S. seaport but that only five percent of U.S.-bound cargo is actually scanned overseas. As for cargo deemed high-risk by CBP, just 85 percent is inspected overseas.

Congress should amend the Act to prohibit DHS from exercising extension authority for the 100% scanning mandate unless port assessments that set forth the obstacles to implementation are completed. DHS should strive to ensure that, at a minimum, all cargo it deems as high-risk for containing radiological or nuclear material is scanned overseas and, once accomplished, should build on such efforts to help achieve the 100 percent scanning mandate.

VIII. Surface Transportation Security Programs *(Secs. 1303, 1304, 1404, 1405, 1512, and 1531)*

In addition to authorizing TSGP and requiring security training for frontline transportation workers, the *9/11 Commission Act* directed DHS to: (1) develop Visible Intermodal Protection and Response (VIPR) teams; (2) field surface transportation security inspectors; (3) develop and implement the National Strategy for Public Transportation Security; and (4) conduct security assessments of public transportation, railroad, and bus systems to determine which require security plans. At its peak, in FY12, there were 37 VIPR teams conducting operations in airports and major transportation hubs to deter and detect suspicious activity across modes. The Administration's FY18 budget calls for reducing the program to eight teams. Currently, there are 260 inspectors regulating compliance across all modes of transportation but, at its peak, in FY11, there were 404 inspectors in the field. In 2010, TSA issued a Transportation Systems Sector-Specific Plan as an annex to the National Infrastructure Protection Plan which fulfilled the Act's requirements for a public transportation strategy.

With respect to the assessment and security plan requirement, on December 16, 2016, TSA published an advance notice of proposed rulemaking with the goal of establishing a "uniform base of vulnerability assessments and security plans for security systems." While publication of this notice represents the biggest step TSA has taken on the mandate, the timeline for full implementation is unclear.

Congress should reject the proposed cuts to the VIPR program and TSA should, by the end of the year, issue a proposed rule to establish a vulnerability assessment and security plan program that reflects stakeholder feedback.

IX. Quadrennial Homeland Security Review *(Sec. 2401)*

DHS, the third-largest Federal department, has a broad range of missions that include protecting our borders, facilitating trade, protecting our waterways, emergency response and recovery, transportation security, cybersecurity, and countering violent extremism. Given the scope of these responsibilities, DHS' priorities, programs, and structure must evolve to confront existing and emerging threats and challenges. To that end, the *9/11 Commission Act* directed DHS to produce, every four years, a unified, strategic framework for homeland security missions and goals, known as the Quadrennial Homeland Security Review (QHSR), to be modeled, in part, after the Department of Defense's Quadrennial Defense Review. The Government Accountability Office (GAO) evaluated the first QHSR, issued in 2012, and suggested strengthening planning and risk management efforts as well as stakeholder engagement. GAO concluded that the 2014 QHSR was an improvement over the earlier version but that it failed to fully document how its analyses were synthesized to generate reproducible results. The 2018 review is underway.

Congress should enact H.R. 1297, the *Quadrennial Homeland Security Review Technical Corrections Act of 2017*, as introduced by Vice Ranking Member Bonnie Watson Coleman (D-NJ) that sets forth a range of modifications to the law to enhance the impact of future reviews on the programs and activities of the Department and its partners in the Homeland Security Enterprise (HSE).

X. Biosurveillance *(Sec. 1101)*

Section 1101 of the *9/11 Commission Act* established the National Biosurveillance and Integration Center (NBIC) to track biological events of national concern, disseminate alerts, and oversee the development of the National Biosurveillance Integration System (NBIS). However, it quickly became unclear whether the NBIC would be capable of fulfilling that purpose due to partner agencies' failure to provide necessary data and personnel. GAO recommended that (1) the NBIC further define its mission, purpose, and coordination methods and (2) establish performance measures to monitor effectiveness and collaboration efforts. In 2015, NBIC continued to face similar issues. The Blue Ribbon Study Panel on Biodefense recommended that authority for Federal biosurveillance and biodefense efforts

be centralized within the White House to incentivize cooperation between agencies. The Administration's FY18 budget proposes the elimination of the NBIC; however, State and local governments, along with the National Security Council have argued that NBIC's work is valuable and that eliminating the program without consulting stakeholders is illogical.

Instead, Congress should direct a review of the NBIC to ascertain its value to Federal, State, and local stakeholders and, at the same time, consider whether aspects of the Center's mission would be better carried out elsewhere in the Federal government. Additionally, the President should designate a high-ranking official in the White House to coordinate Federal biosurveillance and biodefense efforts.

I. HOMELAND SECURITY GRANT PROGRAM *(Sec. 101)*

Background:

Almost immediately after the terrorist attacks of September 11, 2001 (9/11 attacks), the Federal government began funneling money to State and local governments to begin to build a national emergency preparedness and response infrastructure. Between Fiscal Year (FY)03 and FY06, the newly-established Department of Homeland Security (DHS or Department) provided assistance to State and local governments through the following grant programs: (1) State Homeland Security Grant Program (SHSGP); (2) Emergency Management Performance Grant Program; (3) Metropolitan Medical Response System; (4) Law Enforcement Terrorism Prevention Program; (5) Urban Area Security Initiative (UASI); (6) Critical Infrastructure Protection Program; and (7) Citizen Corps Program.[1]

Regarding the provision of this Federal assistance, the National Commission on Terrorist Attacks Upon the United States (9/11 Commission) observed that "a major portion of the billions of dollars appropriated for [S]tate and local assistance is allocated so that each [S]tate gets a certain amount, or an allocation based on its population – wherever they live."[2] Although the Commission acknowledged that "every [S]tate and city needs to have some minimum infrastructure for emergency response," it cautioned that Federal funding "should supplement [S]tate and local resources based on the risks or vulnerabilities that merit additional support."[3] To ensure the most effective use of limited resources, it recommended that "[h]omeland security assistance should be based strictly on an assessment of risks and vulnerabilities."[4]

In response, the *Implementing Recommendations of the 9/11 Commission Act of 2007* (*9/11 Commission Act)* sought to improve how the Department, through the Federal Emergency Management Agency (FEMA), administers the UASI and SHSGP programs. Section 101 directed the FEMA Administrator to "conduct an initial assessment of the relative threat, vulnerability, and consequences from acts of terrorism faced by"[5] the "100 most populous metropolitan statistical areas in the United States"[6] and to make UASI awards based on that

[1] Steven Maguire and Shawn Reese, *Department of Homeland Security Grants to State and Local Governments: FY03 to FY06* (CRS Report No. RL33770) (Washington, DC: Congressional Research Service, 2016), 2-3.The programs that existed prior to the 9/11 attacks that were administered by legacy agencies are: (1) the Metropolitan Medical Response System administered by the Department of Health and Human Services; (2) the State Domestic Preparedness Program administered by the Department of Justice; and (3) the Emergency Management Performance Grant Program administered by the Federal Emergency Management Agency.
[2] U.S. National Commission on Terrorist Attacks upon the United States. *9/11 Commission Report: The Official Report of the 9/11 Commission and Related Publications (9/11 COMMISSION REPORT)*, by Thomas H. Kean and Lee Hamilton, Washington, D.C.: GPO, 2004, 395-96.
[3] *Id*., 396.
[4] Ibid.
[5] Implementing the Recommendations of the 9/11 Commission Act of 2007 (9/11 Commission Act), Pub. L. No. 110-53, 121 Stat. 265, 274 (2007).
[6] *Id*., 121 Stat. 272.

assessment. It also established a threshold for a minimum allocation for SHSGP,[7] but clarified that the FEMA Administrator must allocate funding primarily based on risk.[8] To ensure that UASI and SHSGP awards are informed by an accurate relative risk assessment, the law directed the FEMA Administrator to consider the following factors with respect to a grantee:

> (A) its population, including appropriate consideration of military, tourist, and commuter populations;
> (B) its population density;
> (C) its history of threats, including whether it has been the target of a prior act of terrorism;
> (D) its degree of threat, vulnerability, and consequences related to critical infrastructure (for all critical infrastructure sectors) or key resources identified by the Administrator or the State homeland security plan, including threats, vulnerabilities, and consequences related to critical infrastructure or key resources in nearby jurisdictions;
> (E) the most current threat assessments available to the Department;
> (F) whether the State has, or the high-risk urban area is located at or near, an international border;
> (G) whether it has a coastline bordering an ocean (including the Gulf of Mexico) or international waters;
> (H) its likely need to respond to acts of terrorism occurring in nearby jurisdictions;
> (I) the extent to which it has unmet target capabilities;
> (J) in the case of a high-risk urban area, the extent to which that high-risk urban area includes—
>
> > (i) those incorporated municipalities, counties, parishes, and Indian tribes within the relevant eligible metropolitan area, the inclusion of which will enhance regional efforts to prevent, prepare for, protect against, and respond to acts of terrorism; and
> > (ii) other local and tribal governments in the surrounding area that are likely to be called upon to respond to acts of terrorism within the high-risk urban area; and
>
> (K) such other factors as are specified in writing by the Administrator[.][9]

Since 2002, DHS has invested nearly $50 billion in State and local grant programs to build a stronger national preparedness infrastructure,[10] and the investments have yielded results. Indeed, year after year, FEMA's *National Preparedness Report* shows States have high confidence in the core capability areas that have benefited from grant investments – such as operational coordination, situational assessment, and public alerts and warnings.[11]

---

[7] *Id*., 121 Stat. 278-283.
[8] The Conference Report accompanying the 9/11 Commission Act provides: "In all cases, the minimum is a 'true minimum,' in which funding allocations are initially determined entirely on the basis of terrorism risk and the anticipated effectiveness of the proposed use of the grant. Any recipient that does not reach the minimum based on this risk allocation will receive additional funding from the amount appropriated for the State Homeland Security Grant Program to ensure the respective minimum is met." H. Rep. No. 110-259, at 290 (2007) (Conf. Rep.); Currently, all States, the District of Columbia, and Puerto Rico receive a minimum allocation of 0.36 percent of total allocation, and US territories receive a minimum allocation of 0.08 percent of total allocation. 121 Stat. 278 (2007).
[9] 9/11 Commission Act, 121 Stat. 282 (2007).
[10] U.S. Department of Homeland Security, "DHS Announces Grant Allocations for Fiscal Year 2016 Preparedness Grants," news release, June 29, 2016, https://www.dhs.gov/news/2016/06/29/dhs-announces-grant-allocations-fiscal-year-2016-preparedness-grants.
[11] Federal Emergency Management Agency, U.S. Department of Homeland Security, *National Preparedness Report*, (Washington, DC: March 30, 2016); *National Preparedness Report*, (Washington DC: March 30, 2015); and *National Preparedness Report*, (Washington DC: March 30, 2014).

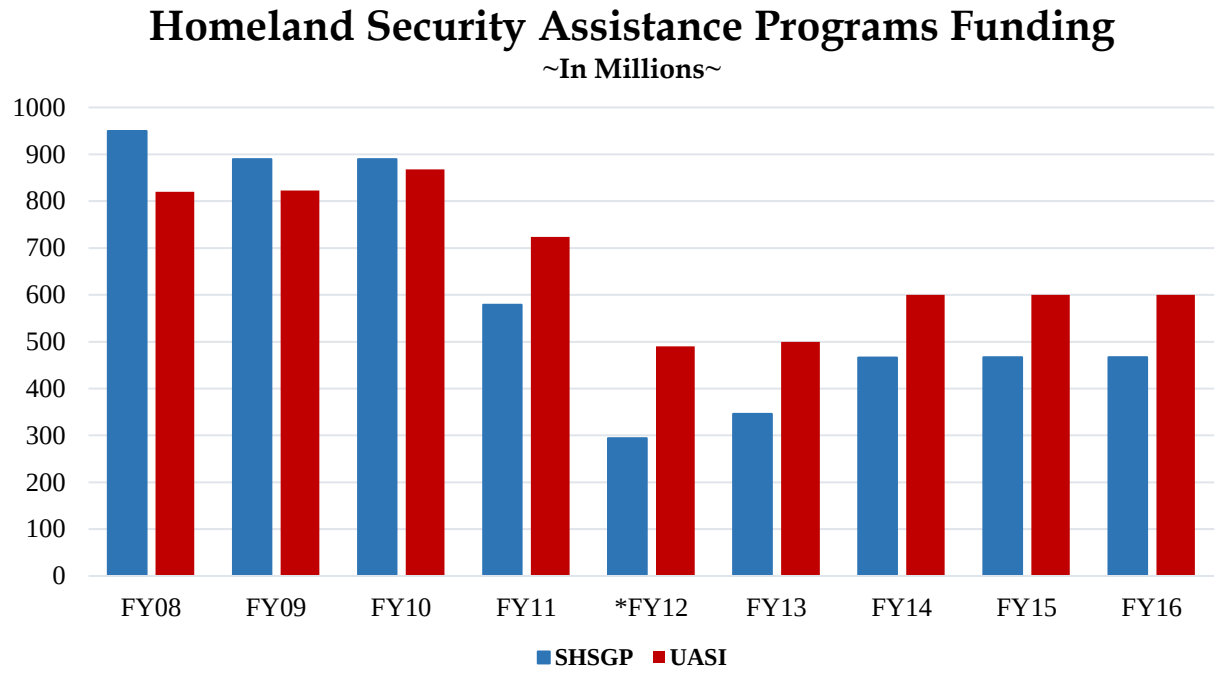
Meanwhile, they have lower confidence in capability areas that receive less funding (e.g.: cyber security and supply chain security).[12]

The response to the April 2013 Boston Marathon Bombings demonstrated how first responder capabilities have improved since the 9/11 attacks. At the House Committee on Homeland Security's hearing on the attack, then-Boston Police Commissioner Ed Davis stated that without grant funding, the "response would have been much less comprehensive than it was" and without the exercises supported through UASI funding, "there would be more people who had died in these -- in these attacks."[13] The Harvard University John F. Kennedy School of Government's Program on Crisis Leadership issued a report in 2014 similarly lauding the role the grants had in facilitating an effective multi-jurisdiction, multi-discipline response to the bombings, observing that "[p]ost-9/11, increased [F]ederal funding for training and exercises, as well as the requirement that most occur at regional scale, contributed to the development of closer institutional relationships."[14] As a result, emergency response leaders "established professional relationships," developed trust and learned to respect the competence of their peers and their agencies, gained an "understanding of complementary capabilities across their respective professional disciplines (e.g., law enforcement, fire service, emergency medical, public health, and hospital-based emergency medicine), and "developed understanding of how best to coordinate and collaborate across agencies."[15]

Under Democratic leadership, homeland security grant programs, including SHSGP and UASI, reached their peak of $2.75 billion in FY10. Unfortunately, starting in FY11, the first year under Republican majorities in the House and Senate, funding for these critical homeland security programs have been drastically reduced. In FY11, when UASI funding was reduced by $850 million to $1.9 billion, 32 cities were removed from the program.[16] The

[12] *National Preparedness Report*, (Washington DC: March 30, 2016), 18.
[13] *The Boston Bombings: A First Look: Hearing before the Comm. on Homeland Security*, *House of Representatives*, 113th Cong. (May 9, 2013) (statement of Edward F. Davis, III, Police Commissioner, City of Boston).
[14] Herman B. "Dutch" Leonard, Christine M. Cole, Arnold M. Howitt, and Philip B. Heymann. "Why Was Boston Strong?: Lessons from the Boston Marathon Bombing." Paper presented at Program on Crisis Leadership, Harvard University John F. Kennedy School of Government, Boston, MA (April 2014), https://ash.harvard.edu/files/why_was_boston_strong.pdf.
[15] Ibid.
[16] Cities eliminated in FY11 include: Albany, NY; Austin, TX; Bakersfield, CA; Baton Rouge, LA; Bridgeport, CT; Buffalo, NY; Columbus, OH; El Paso, TX; Hartford, CT; Honolulu, HI; Indianapolis, IA; Jacksonville, FL; Kansas City, MO; Louisville, KY; Memphis, TN; Milwaukee, WI; Nashville, TN; Oklahoma City, OK; Omaha, NE; Oxnard, CA; Providence, RI; Richmond, VA; Rochester, NY; Sacramento, CA; Salt Lake City, UT; San Antonio, TX; San Juan, PR; Syracuse, NY; Toledo, OH; Tucson, AZ;

following year, Congress appropriated only $1.12 billion to be allocated among 12 homeland security grant programs. Although grant funding was increased to about $1.23 billion in FY13, sequestration further reduced the amount provided to support State and local preparedness and response capabilities. Since FY14, funding for homeland security grants has been level-funded at about $1.3 billion, with around $600 million appropriated for UASI and $460 appropriated for SHSGP.



* FY12 funds were allocated by the DHS Secretary; does not include Administration funds

Findings and Recommendations:

The terrorist threat environment is ever-evolving. The Federal government's policies and programs aimed at protecting communities across the nation must evolve too. With respect to the homeland security grant programs, action on the following **five recommendations** will help ensure that these grants achieve the goals Congress envisioned in the *9/11 Commission Act*: (1) Congress should significantly increase funding for the SHSGP and UASI programs; (2) DHS should evaluate the risk formula and methodology used to allocate grant funds and, as appropriate, make modifications to ensure resources go where they are most needed; (3) Congress should enact legislation to create a competitive funding opportunity for former UASI jurisdictions to maintain capabilities achieved through the program; (4) Congress should authorize the Nonprofit Security Grant Program; and (5) DHS should enhance efforts to help State and local governments improve cybersecurity capabilities.

and Tulsa, OK. Some of these cities, such as Salt Lake City, UT, have been since been funded under the UASI program, while other cities funded in FY11, such as Cincinnati, OH, did not receive a UASI award in FY17.

Funding Levels

Given the ever-evolving threat landscape, support and funding for homeland security grants should be a top priority for Congress. SHSGP and UASI investments have greatly assisted jurisdictions in the development of capabilities to better prevent, protect against, respond to, and recover from acts of terrorism and other incidents. After enactment of the *9/11 Commission Act,* peak funding for SHSGP was in FY08 at $950 million and for UASI was in FY10 at $868 million.[17] However, in recent years, the arbitrary discretionary spending caps imposed by the *Budget Control Act of 2011* have significantly undermined Federal efforts to support critical State and local homeland security preparedness and response.[18]

Funding has remained relatively steady since FY13 but is insufficient to meet State and local emergency responder needs. Rep. Donald Payne, Jr. (D-NJ), the Ranking Member on the Subcommittee for Emergency Preparedness, Response, and Communication offered an amendment during Committee consideration of H.R. 2825, the *Department of Homeland Security Authorization Act of 2017* (*DHS Authorization Act* or H.R. 2825) to authorize SHSGP and UASI at a funding level of $900 million each, up from $600 million and $800 million, respectively, in the base text. Although the amendment was rejected along party lines in Committee, Committee Democrats continue to advocate for robust, reliable funding levels.

Recommendation: Congress should significantly increase funding for the SHSGP and UASI programs.

Risk Formula and Methodology

As former-DHS Secretary John Kelly has said, the nation faces the "highest terror threat level in years" and the "threat has metastasized and decentralized, and the risk is as threatening today as it was that September morning almost 16 years ago."[19] Small and medium-sized cities are increasingly targeted by lone-wolf terrorists and domestic terrorist organizations have become emboldened. In June 2015, for example, a 21-year-old white supremacist opened fire on black parishioners attending Bible study at Emanuel African Methodist Episcopal (AME) Church in Charleston, South Carolina, killing nine people in furtherance of his racist ideology. In August 2017, a white nationalist killed a woman and injured 19 other people in Charlottesville, Virginia, when he drove a car into a group of people counter-

[17] Prior to enactment of the 9/11 Commission Act, SHSGP funding peaked at $1.870 billion in FY03. Shawn Reese, *Department of Homeland Security Preparedness Grants: A Summary and Issues* (CRS Report No. R44669) (Washington, DC: Congressional Research Service, 2016), 16.
[18] In FY17, funding for SHSGP and UASI was $467 million and $605 million, respectively.
[19] John F. Kelly, Secretary of Homeland Security, "Home and Away: DHS and the Threats to America" (speech, George Washington University Center for Cyber and Homeland Security, Washington, DC, April 18, 2017), https://www.dhs.gov/news/2017/04/18/home-and-away-dhs-and-threats-america.

protesting an Alt-Right, white nationalist demonstration. With the emergence of lone wolf attacks in communities that do not participate in the UASI program, there are questions about the extent to which the existing risk formula and methodology is properly targeted to address the threat landscape.

Recommendation: DHS should evaluate the risk formula and methodology used to allocate grant funds and, as appropriate, make modifications to ensure resources go where they are most needed.

Acting through FEMA, DHS should evaluate the risk formula and methodology to ensure that the full spectrum of threats and vulnerabilities are considered and to ensure that the risk assessment is informed by the best information and data. Upon completion of the review, the Department should engage with the stakeholder community and Congress to modernize the risk formula and methodology.

Committee Democrats supported language requiring a review of the risk formula and methodology in the *DHS Authorization Act*. DHS should not wait on enactment of H.R. 2825 to undertake an evaluation of the risk formula and methodology.

Sustainment for Former UASIs

At its peak, over 60 cities received UASI funding. Today, just over 30 cities receive funding. The Committee has heard testimony from State and local first responders that grant reductions negatively impact capabilities.[20] To date, however, a comprehensive assessment of the impacts that homeland security funding cuts or the elimination of funding entirely has had on particular jurisdictions has never been done. To better understand the national preparedness posture, the Department should carry out such an assessment and should provide guidance to assist former UASI jurisdictions on ways to maintain capabilities achieved through previous grant investments.

[20] *The Future of FEMA: Stakeholder Recommendations for the Next Administrator: Hearing before the Subcmte. on Emergency Preparedness, Response, and Communications, Comm. on Homeland Security, House of Representatives*, 115th Cong. (February 14, 2017) (statement of Capt. Chris A. Kelenske, Deputy State Director/Commander, Michigan State Police); *State of Emergency: The Disaster of Cutting Preparedness Grants: Hearing before the Subcmte. on Emergency Preparedness, Response, and Communications, Comm. on Homeland Security, House of Representatives*, 114th Cong. (March 15, 2016) (statements of Hon. Bill de Blasio, Mayor, City of New York, Jim Butterworth, Director, Emergency Management Agency/Homeland Security, State of Georgia, Rhoda Mae Kerr, Fire Chief, City of Austin, Texas, Sgt. W. Greg Kierce, Director, Emergency Management & Homeland Security, City of Jersey City, New Jersey, Mike Sena, Director, Northern California Regional Intelligence Center (on behalf of the National Fusion Center Association), and George Turner, Chief of Police, Atlanta Police Department (on behalf of the Major Cities Chiefs)).

Recommendation: Congress should enact legislation creating a competitive funding opportunity for former UASI jurisdictions to maintain capabilities achieved through the program.

Congress bears responsibility for helping former UASI jurisdictions maintain preparedness capabilities. Committee Democrats have pursued legislation to authorize a competitive grant program to provide former UASI jurisdictions with the resources necessary to maintain capabilities. Rep. Val Demings (D-FL) successfully negotiated a provision with Chairman Michael McCaul (R-TX) to target competitive grant funds to former UASI jurisdictions in the *DHS Authorization Act*.

Non-Profit Security Grants

Since FY07, FEMA has made funding available to secure high-risk nonprofit organizations located within UASI jurisdictions under the Nonprofit Security Grant Program, but the program has never been formally authorized.[21] In the first three months of 2017, there were a spate of threats in 32 States against 71 Jewish Community Centers, five Anti-Defamation League locations, and several Jewish day schools. In recent years, attacks and threats to religious institutions of all faiths have increased dramatically, including at nonprofit locations and places of worship outside of UASI jurisdictions. Attacks include the 2015 Charleston church shooting in which nine parishioners were killed,[22] the 2012 shooting at a Sikh temple in Milwaukee, WI, [23] and the August 5, 2017 improvised explosive device attack on a suburban Minneapolis mosque.[24] According to the Southern Poverty Law Center, the number of active hate groups in the U.S. last year rose to 917 – including 514 anti-Semitic groups, 547 white nationalist groups, and 605 anti-Muslim groups.

Recommendation: Congress should authorize the Nonprofit Security Grant Program.

[21] Authorized in the FY06 Department of Homeland Security (DHS) Appropriations Act and updated in the FY07 DHS Appropriations Act (P.L. 109-295).
[22] Jason Horowitz, Nick Corasaniti, and Ashley Southall, "Nine Killed in Shooting at Black Church in Charleston," *New York Times*, June 17, 2015, https://www.nytimes.com/2015/06/18/us/church-attacked-in-charleston-south-carolina.html?_r=0.
[23] Steven Yaccino, Michael Schwirtz, and Marc Santora, "Gunman Kills 6 at a Sikh Temple Near Milwaukee," *New York Times*, Aug. 5, 2012, http://www.nytimes.com/2012/08/06/us/shooting-reported-at-temple-in-wisconsin.html.
[24] Matt Rehbein, "'Improvised Explosive Device' behind Minnesota Mosque Blast, FBI Says," *CNN*, August 6, 2017, http://www.cnn.com/2017/08/05/us/explosion-reported-minnesota-mosque/index.html.

Congress must act so that Americans can freely exercise their freedom to worship and associate without fear. Congress should enact H.R. 1486, the *Securing American Non-Profit Organizations Against Terrorism Act of 2017*, as introduced by Ranking Member Bennie G. Thompson (D-MS), which would authorize the Non-Profit Security Grant Program and make funding available to non-profit organizations outside UASI jurisdictions. During Committee consideration of the *DHS Authorization Act*, Ranking Member Thompson successfully attached language authorizing the program at $50 million annually. Of that sum, $35 million would be reserved for non-profits within UASI jurisdictions and the remainder would be made available, on a competitive basis, to at-risk non-profits outside UASI jurisdictions.

Cybersecurity Capabilities

Although the United States was largely spared the impacts of recent high-profile ransomware attacks, *WannaCry* and *NotPetya,* our networks are not immune from cybersecurity breaches. Indeed, in June, ISIL hacked State and municipal websites in Ohio, New York, Maryland, and Washington, and displayed ISIL propaganda.[25] There is evidence that prior to the 2016 Presidential elections, Russia targeted the election systems in 21 States, and successfully breached voter databases in a small number of States.[26]

Recommendation: DHS should enhance efforts to help State and local governments to improve cybersecurity capabilities.

Year after year, in the *National Preparedness Report*, States rank cybersecurity as a core capability in which they have the least confidence.[27] Yet, when it comes to decisions about how to expend SHSGP and UASI grants, States generally do not choose to invest in building a robust cybersecurity capability. To better understand the factors that explain this disconnect, Rep. James Langevin (D-RI) offered an amendment during Committee consideration of the *DHS Authorization Act* that directed the FEMA Administrator to conduct a study to inform efforts at improving grant guidance to encourage the use of grant funds to tackle cybersecurity challenges. Although H.R. 2825 has not yet been enacted into law, FEMA should undertake the study in short order. Additionally, the Department, through FEMA, should take a look at whether the resources provided through existing grant programs are sufficient to build robust cybersecurity capabilities at the State and local level and whether a separate, targeted grant program is appropriate. Should FEMA determine a separate grant program is appropriate, FEMA should submit its proposal to Congress.

---

[25] Dakin Adone, et al., "Hack that Plants ISIS Message Hits Another State Government Website," *CNN*, June 27, 2017, http://www.cnn.com/2017/06/26/politics/websites-hacked-isis/index.html.

[26] *Addressing Threats to Election Infrastructure: Hearing before Select Comm. on Intelligence, Senate,* 115th Cong. (June 21, 2017) (Joint testimony of Jeanette Manfra, Acting Deputy Under Secretary for Cyber Security and Communications, National Protection and Programs Directorate, U.S. Department of Homeland Security, and Dr. Samuel Liles, Acting Director, Cyber Division, Office of Intelligence and Analysis, U.S. Department of Homeland Security).

[27] *National Preparedness Report*, (Washington DC: March 30, 2016), 18.

II. INTEROPERABILITY *(Sec. 301)*

Background:

Twenty-one minutes before the North Tower of the World Trade Center collapsed, a police helicopter pilot surveying the collapsed South Tower issued the following warning about the North Tower over the police radio: "'I don't think this has too much longer to go. I would evacuate all people within the area of that second building.'"[28] The message was relayed to police officers and most escaped but it came to light that at least 121 of the firefighters who perished in the North Tower trying to save lives may never have received the warning to evacuate.[29]

Emergency communications failures during the 9/11 attacks costed lives. The communications systems of emergency response agencies were overwhelmed by the amount of users, suffered from weak radio signal strength, and were not interoperable across jurisdictions and across disciplines. These challenges were compounded by the fact that there was no standard operating procedure for how and when responders should access certain channels or communication with response partners.[30] Together, technical and governance challenges undermined the ability of first responders do their jobs safely.

Section 301 of the *9/11 Commission Act* directed the Department to address these interoperability challenges at the State level by creating a grant program, the Interoperable Emergency Communications Grant Program (IECGP), and conditioned grant funding on compliance with State-specific governance plans (Statewide Communications Interoperability Plans) and the National Emergency Communications plan.[31]

[28] Jim Dwyer, Kevin Flynn, and Ford Fessenden, "FATAL CONFUSION: A Troubled Emergency Response; 9/11 Exposed Deadly Flaws in Rescue Plan," *The New York Times*, July 7, 2002, http://www.nytimes.com/2002/07/07/nyregion/fatal-confusion-troubled-emergency-response-9-11-exposed-deadly-flaws-rescue.html?mcubz=0.

[29] Ibid.; It is important to note that the 9/11 Commission found that, despite emergency communications challenges, "*at least* 24 of the *at most* 32 companies who were dispatched to and actually in the North Tower received the evacuation instruction – either via radio or directly from other first responders," and concluded that the "technical failure of FDNY radios, while a contributing factor, was not the primary cause of the many firefighter fatalities in the North Tower." 9/11 COMMISSION REPORT, 322-3.

[30] 9/11 COMMISSION REPORT, 292-3.

[31] The National Emergency Communication Plan was mandated pursuant to the Post-Katrina Emergency Management Reform Act of 2006, 6 U.S.C. § 572 (2006).

Under the law, States would be provided risk-based funding to enhance communications capabilities at the State and local level and each State was guaranteed a minimum allocation. The law required that each State submit a Statewide Communications Interoperability Plan (SCIP) for approval to the Department's Director of Emergency Communications and align grant investments with the SCIP. Grantees were permitted to use the funding for planning, training, exercises, and equipment that met voluntary consensus standards. Between FY08 through FY11, Congress appropriated $50 million annually to IECGP, but under the Republican-controlled Congress, funding for the program was eliminated in FY12.

Prior to the issuance of initial IECGP awards, however, the Department had to produce a National Emergency Communications Plan (NECP) with the dual purpose of supporting the ability of responders to continue to communicate in the event of natural disasters, acts of terrorism, and other man-made disasters and ensuring, accelerating, and attaining interoperable emergency communications nationwide.[32] The first NECP was released in 2008 and an updated version was released in 2014.

The 2008 NECP recognized that interoperability challenges could not be resolved by technology alone and emphasized "coordination, governance, planning, usage, training and exercises at all levels of government."[33] In particular, it identified governance as undermining interoperable emergency communications and encouraged States to designate Statewide Interoperability Coordinators (SWICs), Regional Emergency Communications Coordination Working Groups, State Interoperability Executive Committees, and other governance structures to implement SCIPs and effectively address interoperable communications challenges.[34] By the time the 2014 NECP update was released, 90 percent of the 2008 plan's milestones had been achieved.[35] The 2014 NECP leveraged the progress made and provided updated guidance to accommodate the budget environment, the evolution of technology, and the enactment of legislation authorizing the Public Safety Broadband Network.[36]

---

[32] The Post-Katrina Emergency Management Reform Act of 2006, 6 U.S.C. § 572 (2006).
[33] U.S. Department of Homeland Security, *National Emergency Communications Plan*, (Washington, DC: July 2008), https://www.dhs.gov/xlibrary/assets/national_emergency_communications_plan.pdf
[34] *Id.* 11-12.
[35] U.S. Department of Homeland Security, *National Emergency Communications Plan*, (Washington, DC: 2014), 4, https://www.dhs.gov/sites/default/files/publications/2014%20National%20Emergency%20Communications%20Plan_October%2029%202014.pdf.
[36] Ibid.

Five years after the Department released the first NECP, the Boston Marathon bombings occurred. The strong multi-jurisdiction, multi-discipline, response was attributed largely to the emergency communications infrastructure established pursuant to NECP guidance and gains achieved with IECGP resources.[37] Previously, in 2010, DHS made a series of recommendations to the region's first responder community based on its observations during the Boston Marathon. Subsequently, with IECGP money, the Boston region worked to address the issues identified by DHS, including training additional Communications Unit Technicians (COMTs).[38] According to Steve Staffier, the SWIC for Massachusetts at the time of the 2013 Boston Marathon bombings: "'[T]he key to our success is that we have the State communications unit team, which is made-up of [Communications Unit Leaders], COMTs, and all of the subject matter experts who run these radio systems.'"[39] Moreover, he observed that planning "'is more key than anything money can buy as far as systems and technology.'"[40]

A related communications challenge identified by the 9/11 Commission was the need for "expedited and increased assignment of radio spectrum for public safety use."[41] In response, Congress passed the *Public Safety and Spectrum Act* in 2012 to direct the establishment of the First Responder Network Authority (FirstNet), a public safety broadband network on dedicated spectrum.[42] That law authorized $7 billion in funding to build out the network, supported in part by proceeds from spectrum auctions. It also directed that, by 2023, public safety users be required to relocate from the T-Band spectrum, an important emergency communications spectrum resource.[43] Currently, the following jurisdictions rely on T-Band spectrum: Boston, Chicago, Dallas, Houston, Los Angeles, Miami, New York, Philadelphia, Pittsburgh, San Francisco, and Washington, D.C.[44]

Findings and Recommendations

Governance

Despite gains in interoperable communications, continued focus on closing operational challenges and overcoming governance gaps is needed. This point was underscored in a quote shared, in testimony before the Committee, by the Chairman of the National Council of Statewide Interoperability Coordinators (NCSWIC) from the former Massachusetts SWIC, Steve Staffier:

> As I witnessed during the Boston Marathon Bombings, even though we have all made significant investments in equipment and systems around the

[37] Office of Emergency Communications, U.S. Department of Homeland Security, *Emergency Communications Case Study: Emergency Communications During the Response to the Boston Marathon Bombing*, (Washington, DC: April 2013), https://www.dhs.gov/sites/default/files/publications/oec-case%20study-support%20for%20response%20to%20boston%20marathon%20bombing-2013.pdf.
[38] Ibid.
[39] Ibid.
[40] Ibid.
[41] Ibid.
[42] Middle Class Tax Relief and Job Creation Act of 2012, Pub. L. No. 112-96, 126 Stat. 206 (2012).
[43] Ibid.
[44] "T-Band Update Report: 2016," National Public Safety Telecommunications Council, (May 31, 2016) 3, http://npstc.org/download.jsp?tableId=37&column=217&id=3696&file=T_Band_Update_Report_Final.pdf.

> country, we still need help in education/training/outreach to the end users and key decision makers…and this requires a SWIC and funding. These radios and systems don't talk on their own and the coordination doesn't happen without the SWIC and a COMU (Communications Unit) Team of COML's (Certified Communication Leaders) and COMT's (Certified Communication Technicians).[45]

The NCSWIC Chairman went on to explain that interoperability is "really about people in disparate agencies and jurisdictions including each other in their planning processes."[46] IECGP funds supported the governance structures that facilitated advances in interoperability, including dedicated SWICs. As a result of the program's elimination, today, many States no longer have a dedicated SWIC. The contributions that SWICs make to State emergency communications are manifold. Not only do SWICs facilitate the development of SCIPs and emergency communications plans, they save States money by ensuring that emergency communications investments are coordinated and compatible. The elimination of the IECGP in FY12 was a major setback for interoperability efforts.

Recommendation: Congress must provide new resources to States to support interoperability efforts and help ensure that the critical work that SWICs perform and governance structures that facilitate interoperability continue.

Effective governance structures are the backbone of interoperability. In the 114th Congress, Rep. Donald Payne, Jr. (D-NJ) introduced legislation, the *Statewide Interoperable Communications Enhancement Act* to require States to designate a SWIC or certify that SWIC activities were being carried out in some other fashion. The bill sought to ensure that States do not lose ground on the progress made toward developing interoperable emergency communications capabilities. In the future, Congress should prioritize emergency communications governance structures and ensure that sufficient grant funding is available to help States pay for them.

[45] *Interoperable Communications: Accessing Progress Since 9/11*, *Hearing before Subcmte. on Emergency Preparedness, Response, and Communications*, *Comm. on Homeland Security*, *House of Representatives*, 113th Cong. (November 18, 2014) (statement of Mark A. Grubb, Director, Delaware Division of Communications on behalf of the National Council of Statewide Interoperability Coordinators).
[46] Ibid.

T-Band

The Federal Communications Commission is required to begin auctioning off the T-Band spectrum used by certain public safety agencies by 2021 and to remove all public safety agencies from the spectrum by 2023.[47] Presently, it is unclear whether the Public Safety Broadband Network will be capable of providing mission critical voice capabilities to public safety users by 2023. Regarding the possibility of public safety users will have to relocate from the T-Band, New York City Mayor Bill de Blasio testified that:

> T-Band is a critical part of the work we do in terms of emergency communications. Disrupting that reality could prove to be very dangerous. We have, as you know, a very highly developed apparatus in New York City to protect our people and protect again the 60 million people who visit every year. It has to do with a number of agencies constantly working together in a very crowded complex environment and the current communications structure allows us to do that work. If Congress doesn't act and we have to relinquish the current approach, we fear a situation that's really disruptive.[48]

Fire Chief Gerald R. Reardon from the City of Cambridge, Massachusetts, similarly expressed concern that forcing first responder agencies to relocate off the T-Band would result not only in millions of dollars in sunk costs, but also lost capabilities. In particular, the Boston Area Police Emergency Radio Network, which was used by responding law enforcement agencies during the Boston Marathon Bombings, is currently used by 166 law enforcement agencies from the New Hampshire border to Cape Cod Canal. That network is on the T-Band.[49]

Recommendation: Congress must allow for public safety organizations that rely on the T-Band to remain on this spectrum until mission critical voice capabilities on the Public Safety Broadband Network are available.

[47] *Supra*, note 42.
[48] *State of Emergency: The Disaster of Cutting Preparedness Grants, Hearing before the Subcmte. on Emergency Preparedness, Response, and Communications, Comm. on Homeland Security, House of Representatives*, 114th Cong. (March 15, 2016) (statement of Hon. Bill de Blasio, Mayor of New York City).
[49] *Supra*, note 44 at 6.

III. INFORMATION SHARING *(Secs. 501 and 511)*

Background:

In April, 2017, then-DHS Secretary Kelly explained why we still "face the highest terror threat level in years" as follows:

> For a brief moment after the attacks of 9/11, our nation shook off its complacency, and realized our American values had a mortal enemy called radical Islam. But as the years have passed we've grown complacent protected by the effectiveness of our worldwide intelligence collection, and the heroics of all those in uniform including our military, local law enforcement, and the men and women of DHS.
>
> The threat to our nation and our American way of life has not diminished. In fact, the threat has metastasized and decentralized, and the risk is as threatening today as it was that September morning almost 16 years ago.[50]

Effective information sharing is critical to addressing the "metastasized and decentralized" threats that our nation faces. The 9/11 attacks exposed serious information sharing gaps within the Federal government and between the Federal government and State, local, tribal, and territorial (SLTT) partners. Over the past sixteen years, policies and procedures have been reformed at all levels to ensure that critical national security information is shared. These reforms have been achieved through the promulgation of Executive Orders, legislation, and the issuance of internal agency policies.

With respect to the DHS' information sharing enterprise, the *9/11 Commission Act* included a number of mandates. Two noteworthy provisions were section 501, which directed the DHS Secretary to reform the Department's terrorist threat or risk advisory system, and section 511, which required the DHS Secretary to establish a State, local, and regional fusion center initiative.

Terrorist Threat Warning System

One of the earliest efforts at fostering greater information sharing about the terrorism risks was the creation of the Homeland Security Advisory System (HSAS).[51] In March 2002, then-Office of Homeland Security Director Tom Ridge unveiled the HSAS as a platform to provide advisories or warnings to SLTT and private sector partners about the threat of an act of terrorism on U.S. soil. The HSAS was a color-coded system and had five threat levels: low-"green", guarded-"blue", elevated-"yellow", high-"orange", and severe-"red". In the eight

[50] *Supra*, note 19.
[51] Homeland Security Presidential Directive 3 (March 11, 2002), https://georgewbush-whitehouse.archives.gov/news/releases/2002/03/20020312-5.html.

years that the HSAS operated, the threat level was never lowered below elevated-"yellow" but was changed 17 times[52] with the level raised to severe-"red" only once.[53] In 2005, the Congressional Research Service warned that "a number of issues have arisen [with the HSAS system], among which are: the vagueness of warnings disseminated by the system; the system's lack of protective measures recommended for state and local governments, and the public; the perceived inadequacy of disseminating threats to state and local governments, the public, and the private sector; and how to best coordinate HSAS with other existing warning systems."[54]

To address the HSAS's weaknesses, section 501 of the *9/11 Commission Act* required the DHS Secretary to modify the system to (1) establish criteria for the issuance and revocation of advisories or warnings; (2) develop a methodology, relying on the established criteria, for advisories and warnings to be issued and revoked; (3) provide, in each advisory or warning, specific information and advice on protective measures at maximum level of detail practical; (4) when possible, limit the scope of each advisory or warning to a specific region, locality or economic sector; and (5) not use color designations alone to specify homeland security threat conditions.

On April 26, 2011, in response to this statutory mandate as well as recommendations issued in September 2009 by a Homeland Security Advisory Council Task Force,[55] then-DHS Secretary Janet Napolitano replaced the HSAS with the National Terrorism Advisory System (NTAS).[56] Under this new system, alerts were only to be issued in the event of "elevated" or "imminent" threats, and alerts would automatically expire after two weeks unless information about the threat necessitated otherwise. An "elevated" alert would be issued to warn of "a credible threat against the United States" while an "imminent" alert would be issued to warn of "a credible, specific, and impending terrorist threat against the United States."[57] In the first four years of the NTAS system, not a single alert was issued by the Department, as the threshold that "a specific, credible terrorist threat to the homeland"[58] exist was never met.[59]

Subsequently, on December 16, 2015, then-DHS Secretary Jeh Johnson announced the addition of a bulletin feature to the NTAS to allow DHS to communicate critical terrorism

---

[52] Jessica Zuckerman, "National Terrorism Threat Level: Color-Coded System Not Missed," *Heritage Foundation*, (September 26, 2012), http://www.heritage.org/homeland-security/report/national-terrorism-threat-level-color-coded-system-not-missed.
[53] On August 10, 2006, the threat level was raised to severe-"red" for commercial flights from the United Kingdom to the U.S., after British authorities announced that a major terrorist plot to blow up an aircraft had been disrupted.
[54] Shawn Reese, *Homeland Security Advisory System: Possible Issues for Congressional Oversight* (CRS Report No. RL32023) (Washington, DC: Congressional Research Service, 2005), 4.
[55] Homeland Security Advisory Council. *Homeland Security Advisory System: Task Force Report and Recommendations*, Washington, DC, by Frances Fragos Townsend and William Webster, September 2009, https://www.dhs.gov/xlibrary/assets/hsac_final_report_09_15_09.pdf.
[56] U.S. Department of Homeland Security, "Secretary Napolitano Announces Implementation of National Terrorism Advisory System," news release, April 20, 2011, https://www.dhs.gov/news/2011/04/20/secretary-napolitano-announces-implementation-national-terrorism-advisory-system.
[57] Ibid.
[58] *Ten Years After 9/11: Are We Safer?: Hearing before Comm. on Homeland Security and Governmental Affairs, Senate*, 112th Cong. (September 13, 2011) (statement of Janet Napolitano, Secretary of Homeland Security).
[59] Rebecca Shabad, "Jeh Johnson: DHS modifies terror alert system," *CBS News*, December 16, 2015, http://www.cbsnews.com/news/dhs-introduces-modification-to-the-terror-alert-system/.

information quickly to homeland security partners and the public that would not warrant the issuance of an alert. To date, DHS has, on four occasions, broadly circulated one-page bulletins with information on trends and developments related to terrorism within the U.S.; each bulletin is in effect for a six-month period.[60]

Fusion Centers

In 2004, the 9/11 Commission predicted that the nascent Department of Homeland Security "will play an important part" in establishing reciprocal relationships between Federal, State, and local partners in which "state and local agents understand what information they are looking for and, in return, receive some of the information being developed about what is happening, or may happen, in their communities."[61] To put DHS on the path to becoming an important partner to SLTT, section 511 of the *9/11 Commission Act* directed the establishment of a State, local, and regional fusion center initiative.

Fusion centers are regional, State, or major urban area level analysis centers where representatives from multiple Federal, State, and local agencies from the law enforcement, first responder, emergency management, and the private sector co-locate to share information in real time and, ultimately, improve information flow to prevent terrorism and other crime. Each fusion center is owned and operated by State and local entities, and is designated by its respective governor. Section 511 requires DHS to support Federal efforts to integrate fusion centers into the Information Sharing Environment,[62] assign personnel to centers, incorporate fusion center intelligence information into DHS information, provide training, and facilitate close communication and coordination between the Department and the centers. DHS, working with the Department of Justice, has developed guidelines for the centers that address performance, privacy, and governance.

The support DHS provides is multifaceted and includes the provision of the Office Intelligence and Analysis (I&A) analysts and report officers on a temporary basis (i.e. detailees), as well as the provision of technical assistance and equipment, including the installation of classified Homeland Secure Data Network (HSDN) terminals within centers. Within DHS, I&A spearheads the Department's support for the 79 centers across the country that have come to be known as the National Network of Fusion Centers.[63] I&A deploys DHS personnel with operational and intelligence skills to the centers to facilitate coordination and the flow of information between DHS and fusion centers, and help maintain local situational awareness about threats. Today, these centers are the primary vehicle for the dissemination of I&A intelligence products and those generated by other Federal agencies.

---

[60] The four bulletins were issued on: December 16, 2015, June 15, 2016, November 15, 2016, and May 15, 2017, https://www.dhs.gov/national-terrorism-advisory-system.

[61] 9/11 COMMISSION REPORT, 427.

[62] The "Information Sharing Environment" is an overarching approach to strengthening the sharing of intelligence, terrorism, homeland security, law enforcement, and other information among Federal, State, local, tribal, international, and private sector partners.

[63] U.S Department of Homeland Security, "Fusion Center Locations and Contact Information," last modified August 9, 2017, accessed August 22, 2017, https://www.dhs.gov/fusion-center-locations-and-contact-information.

Fusion centers receive direct Federal grant funds as well as investment funds. In FY15, fusion centers received $63.7 million in Federal grants, a decrease of 13% percent or $9.8 million from FY14.[64] In FY15, DHS deployed 244 staff to fusion centers, the most by any one Federal partner.[65] Additionally, since FY11, I&A has collaborated with FEMA to ensure that each fusion center's grant application includes an investment justification that explains how funds would advance or maintain information sharing capabilities for that State or urban area.

Findings & Recommendations:

Since the 9/11 attacks, information sharing regarding terrorism threats has improved, in part, due to implementation of the *9/11 Commission Act*. Today, there are numerous channels for the sharing of threat information at multiple levels; the channels include NTAS bulletins that push out timely threat stream information to the public, a web-based platform where Sensitive But Unclassified Information is accessed by appropriate officials (the Homeland Security Information Network (HSIN)), and the classified Homeland Secure Data Network on which analysts with security clearances access Secret-level terrorism-related information at fusion centers.

Recommendation: Looking ahead, DHS should endeavor to ensure that the information sharing programs and intelligence products are responsive to feedback from SLTT and private sector stakeholders.

Over the past decade, I&A has prioritized helping SLTT participate in fusion centers by sponsoring and funding security clearances for SLTT personnel. To date, 91.6% of all SLTT personnel located at fusion centers who need clearances have active clearances.[66] Of the remaining personnel who need clearances, 6.3% have requests pending. As a result, every fusion center has at least one staff member with a clearance at the Secret level or above.[67]

Recommendation: DHS should continue to support fusion centers, including by sponsoring clearances, and work to identify and remove obstacles to the timely sharing of terrorist threat information.

[64] *2015 National Network of Fusion Centers: Final Report*, (Washington, DC, April 2016), 8, https://www.archives.gov/files/isoo/oversight-groups/sltps-pac/national-network-of-fusion-centers-2015.pdf.
[65] Ibid.; The Department of Justice provided 111 staff and other Federal agency provided 10 staff.
[66] *2015 National Network of Fusion Centers: Final Report*, (Washington DC: April 2016), 10.
[67] Ibid.

DHS should continue to work to foster an environment in which the National Network can grow and adapt as the nature of threats, incidents, and response change. At the same time, it is essential that consistent oversight be conducted by Congress, DHS, the Government Accountability Office (GAO), and other Federal watchdogs to ensure that fusion centers comport with Federal performance, privacy, and governance guidelines, and contribute to efforts to prevent terrorism and other crimes.

A concern for the future of National Network is a sentiment among some that these centers are redundant with the Federal Bureau of Investigation's Joint Terrorism Task Forces (JTTFs). Fusion centers and task forces, specifically JTTFs, serve complementary but distinct roles. A fusion center is a "collaborative effort of two or more Federal, State, local, or tribal government agencies that combines resources, expertise, or information with the goal of maximizing the ability of such agencies to detect, prevent, investigate, apprehend, and respond to criminal or terrorist activity."[68] While fusion centers are generally focused on situational awareness and homeland security threats, FBI task forces are more operational in nature—focused on carrying out law enforcement investigations or operations to counter specific threats such as gang violence or online fraud. Further, fusion centers serve as focal points within the State and local environment for the receipt, analysis, gathering, and sharing of threat-related information from Federal and SLTT partners. Fusion centers produce actionable intelligence for dissemination, which can aid other law enforcement organizations, including the JTTFs, in their investigative operations. The distinctions between fusion centers and JTTFs are not only important, but intentional.

With respect to the terrorism threat alert system, DHS has effectively moved past the dismal failure of the HSAS color-coded system. That system stirred fear, confusion and loathing as it was incapable of providing any rationale for adjustments to threat levels or guidance on what actions should be taken to address the threat. NTAS, the successor program that was launched in 2011 pursuant to the *9/11 Commission Act*, was responsive to the HSAS' shortcomings but came to be seen as too rigid with its "specific, credible terrorist threat to the homeland" threshold.[69] Given the dynamic threat picture, it is troubling that it took DHS another four years to identify a modification to the system that rendered it usable. The addition of the bulletin feature to the NTAS in 2015 appears to provide the public and homeland security stakeholders with greater clarity about the threat environment.

[68] Program Manager, Information Sharing Environment, Office of the Director of National Intelligence, *Information Sharing Environment Implementation Plan*, (Washington, DC: November 2006), 119, https://www.ise.gov/sites/default/files/ise-impplan-200611.pdf.
[69] *Supra*, note 59.

Recommendations: The Department should (1) seek feedback to ensure that the system is timely and relevant as terrorist threats continue to evolve; (2) develop metrics to measure the effectiveness of the system; (3) refine the system, as appropriate, based on stakeholder feedback; and (4) continue to expand the visibility of NTAS bulletins or alerts among the public.

IV. MODERNIZATION OF THE VISA WAIVER PROGRAM/ BIOMETRIC ENTRY-EXIT SYSTEM *(Sec. 711)*

Background:

Generally, foreign nationals who wish to travel to the U.S. must obtain a visa for admission. However, since 2000, nationals from certain countries, many of which are in Europe, have been able to travel to the U.S. without a visa for up to 90 days for business or tourism under the Visa Waiver Program (VWP).[70] Today, there are 38 VWP-designated countries[71] and by fiscal year 2014, about 30% of all temporary visitors (21 million visitors) to the U.S. traveled under VWP.[72] Following the 9/11 attacks, there was broad recognition that this important travel and tourism facilitation program needed to be modernized to prevent terrorists from exploiting the program to bypass visa screening.

The 9/11 Commission report noted that none of the terrorists that carried out the attacks entered the U.S. under VWP but recommended that DHS "complete, as quickly as possible, a

[70] Visa Waiver Permanent Program Act, Pub. L. No. 106-396, 114 Stat. 1637 (2000).
[71] Currently, the 38 VWP-designated countries are: Andorra, Australia, Austria, Belgium, Brunei, Chile, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Monaco, Netherlands, New Zealand, Norway, Portugal, San Marino, Singapore, Slovakia, Slovenia, South Korea, Spain, Sweden, Switzerland, Taiwan, and the United Kingdom.
[72] Alison Siskin, *Visa Waiver Program* (CRS Report No. RL32221) (Washington, DC: Congressional Research Service, 2016), 11.

biometric entry-exit screening system."[73] In response to this recommendation, section 711 of the *9/11 Commission Act* required that the DHS Secretary, by August 3, 2008, establish a biometric exit system that records the departure of VWP visitors traveling by air.[74] Further, to modernize the VWP program, section 711 mandated that the DHS Secretary develop and implement an electronic travel authorization system through which each foreign national electronically provides, in advance of travel, biographical information necessary to determine whether the individual is eligible to travel to the U.S. under VWP.[75] The system, as implemented, is known as the Electronic System for Travel Authorization (ESTA), and became fully operational for all VWP visitors traveling to the U.S. by airplane or cruise ship on January 12, 2009.[76]

Electronic System for Travel Authorization

The establishment of the ESTA program modernized VWP and, for the first time, gave U.S. Customs and Border Protection (CBP) the ability to determine whether a foreign national of a VWP-designated country represents a law enforcement or security risk before traveling to the U.S. Today, once an individual submits an ESTA application, CBP vets the individual's information against several databases, including the FBI's Terrorist Screening Database and INTERPOL's Stolen and Lost Travel Documents Database.[77] If the ESTA application is approved, the individual is authorized to travel to the U.S. for up to 90 days, on multiple occasions, for two years (or until the person's passport expires). Those whose applications are denied are referred to a U.S. embassy or consulate to complete the visa application process.[78] In 2015, the DHS Secretary was granted the authority to shorten the validity period of any ESTA determination, or revoke the determination at any time for any reason.[79] Notably, a determination under ESTA that an individual is eligible to travel to the U.S. under VWP does not constitute a determination that the person is admissible. At U.S. ports of entry, CBP Officers interview, fingerprint, and photograph VWP visitors as well as foreign nationals admitted under visas to verify identity and vet travel documents and fingerprints against various U.S. biometric databases to determine admissibility.

Biometric Entry-Exit Program

Currently, CBP's system for tracking the entries and exits of foreign visitors relies primarily on *biographic* data from the visitor's visa or ESTA application. CBP's collection of *biometric* information (fingerprints and photographs) on foreign nationals primarily happens upon

[73] 9/11 COMMISSION REPORT, 389; Starting in 1996, statutory mandates for the creation of an entry-exit system to, in part, help immigration officials positively identify foreign nationals in the United States who had overstayed their visas had been in law.
[74] 9/11 Commission Act, 121 Stat. 338 (2007).
[75] Ibid.
[76] *Supra*, note 72 at 11.
[77] *Visa Waiver Program: DHS Should Take Steps to Ensure Timeliness of Information Needed to Protect U.S. National Security* (GAO-16-498) (Washington, DC: U.S. Government Accountability Office, 2016), 6, https://www.gao.gov/assets/680/676948.pdf.
[78] Ibid.
[79] Consolidated Appropriations Act, Pub. L. No. 114-113, 129 Stat. 2994 (2015).

entry to the U.S. A corresponding system to collect biometrics upon exit or departure has not been deployed as mandated under section 711 of the *9/11 Commission Act*.

Over the past thirteen years, DHS has carried out multiple pilots in pursuit of an exit capability but, to date, limitations related to infrastructure, travel environments, and technology have stood in the way of DHS achieving a biometric exit capability.[80] Four of these pilot programs have been described by GAO as problematic, and have been discontinued; but two programs (involving biographic information sharing with air carriers and with the government of Canada) have been described by DHS as successful, and are ongoing.[81]

In 2016, Congress authorized $1 billion to be collected through fees over ten years for DHS to implement a biometric exit system.[82] Then-DHS Secretary Johnson committed to implementing a system at airports by 2018[83] and in early 2017, President Trump issued an Executive Order that called for a biometric exit system to be implemented.[84]

CBP plans to (1) deploy a biometric exit system that is capable of accepting camera devices and processing transactions in the air environment by 2018; (2) reengineer its entry system; and (3) identify an exit technology for land border crossings by FY21.[85] Furthermore, CBP has a development and deployment schedule to incrementally achieve progress toward a fully-integrated biometric system by 2025.[86]

Foreign nationals who are legally admitted to the U.S. on a temporary basis, but fail to depart when their visas expire, are often referred to as "overstays."[87] DHS identifies two types of overstays – those individuals for whom no departure has been recorded (Suspected In-Country Overstay) and those whose departure was recorded after their lawful admission period expired (Out-of-Country Overstay).[88] Five of the 9/11 terrorists were visa overstays, thus, overstays are a concern not only for immigration control but also for homeland security.[89]

Overstay rates are critical data points that underpins both VWP and the biometric entry-exit system. Starting in 2015, the Department was required to annually report to Congress

[80] Lisa Seghetti, *Border Security: Immigration Inspections at Ports of Entry* (CRS Report No. R43356) (Washington, DC: Congressional Research Service, 2015), 11-12.
[81] Ibid.
[82] Consolidated Appropriations Act, Pub. L. No. 114-113, 129 Stat. 3006 (2015).
[83] U.S. Department of Homeland Security, *Comprehensive Biometric Entry/Exit Plan, Fiscal Year 2016 Report to Congress* (Washington, DC: April 20, 2016).
[84] Exec. Order No. 13769, (March 6, 2017), https://www.whitehouse.gov/the-press-office/2017/03/06/executive-order-protecting-nation-foreign-terrorist-entry-united-states.
[85] *Visa Overstays: A Gap in the Nation's Border Security: Hearing before the Subcommittee on Border and Maritime Security, Comm. on Homeland Security, House of Representatives*, 115th Cong. (May 23, 2017) (joint statement of John Wagner, Deputy Executive Assistant Commissioner, U.S. Customs and Border Protection, Clark Settles, Assistant Director for National Security Division, Homeland Security Investigations, and Michael Dougherty, Acting Assistant Secretary for Border, Immigration, and Trade, Office of Policy, U.S. Department of Homeland Security).
[86] U.S. Customs and Border Protection: Briefing with H. Comm. on Homeland Security Majority and Minority staff (July 18, 2017).
[87] U.S. Department of Homeland Security, *Fiscal Year 2016 Entry/Exit Overstay Report*, (Washington, DC: May 22, 2017), 8.
[88] Ibid.
[89] U.S. Department of Homeland Security, *Entry/Exit Overstay Report: Fiscal Year 2015* (Washington, DC: January 19, 2016), iii.

information on departures and overstays, by country.[90] On May 22, 2017, DHS issued its second annual Entry/Exit Overstay Report, which provided data on foreign visitors who were admitted into the U.S. as nonimmigrants through air and sea ports of entry (POEs) and were expected to depart in FY16. DHS reported that approximately 50.4 million nonimmigrant visitors admitted to the U.S. through air or sea POEs were expected to depart in FY16, which is an increase over the 44.9 million estimate submitted in FY15.[91] Of this number, an estimated 739,478 individuals are suspected to have overstayed their visas, representing 1.47 percent of nonimmigrant visitors,[92] which indicates an increase of 212,351 overstays over the FY15 level. In other words, DHS believes that 0.30 percent fewer nonimmigrant visitors complied with their terms of admission in FY16 than in FY15.[93] For VWP countries, the FY16 Suspected-In-Country overstay rate was 0.60 percent of the approximately 21.6 million expected departures.[94] For non-VWP countries, the FY16 Suspected-In-Country overstay rate was 1.9 percent of the approximately 13.9 million expected departures.[95]

Findings & Recommendations:

While CBP, in recent years, has made progress towards achieving an integrated biometric entry-exit system for the air environment and has told Congress that it is on a trajectory to have it in place by the end of FY18, significant operational challenges and policy questions remain.

Partnership with airline and industry stakeholders is critical to the successful deployment of a biometric exit system as, today, CBP relies heavily on airline partners and their

[90] Consolidated Appropriations Act, Pub. L. No. 114-113, 129 Stat. 2493 (2015).
[91] *Fiscal Year 2016 Entry/Exit Overstay Report*, (Washington, DC: May 22, 2017), 13.
[92] Ibid.
[93] Ibid.
[94] Ibid.
[95] Ibid.

personnel to assist in collecting biometrics from departing passengers. Without airline personnel assisting in biometric data collection, CBP estimates it will need roughly 1,200 additional CBP Officers (CBPOs) to implement the biometric exit capability in addition to the 3,500 CBPOs that it currently needs to address shortages in the Office of Field Operations (OFO). CBP's OFO staffing challenges are exacerbated by the fact that the Department, through policy and budget requests, has prioritized other enforcement functions ahead of the already escalating staffing needs of POEs.

Recommendation: DHS should immediately prioritize CBP Officer staffing at airports and other POEs to foster not only greater travel and trade facilitation but enhance border security.

It is important to recognize that while airlines and industry partners have played a significant role in the recent progress toward a biometric system, the responsibility for implementing this border security program ultimately rests with DHS.

Any system CBP employs to collect biometric exit data must be consistent with existing privacy laws and regulations and safeguard the privacy of U.S. citizens and legal permanent residents. Today, CBP is pursuing the Traveler Verification Service (TVS), an approach where biometric data is collected from all air departing international passengers; it introduces privacy challenges insofar as images of U.S. citizens and legal residents are captured together with foreign nationals.

On August 1, 2017, CBP held the first of numerous engagements planned with privacy groups to discuss the program.[96] Within days, the American Civil Liberties Union cautioned that the TVS system "raises very serious privacy issues."[97] It is critical that constructive engagement be maintained with the privacy community to resolve concerns, as the December 2018 target nears.

Recommendation: CBP and the Department's Privacy Officer should continue to actively engage with the privacy community about the biometric exit program.

[96] U.S. Customs and Border Protection, "CBP Meets with Privacy Groups to Discuss Biometric Exit," news release, August 1, 2017, https://www.cbp.gov/newsroom/national-media-release/cbp-meets-privacy-groups-discuss-biometric-exit.
[97] Jay Stanley, "What's Wrong with Airport Facial Recognition?" *American Civil Liberties Union*, (August 4, 2017), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/whats-wrong-airport-face-recognition?redirect=blog/free-future/whats-wrong-airport-face-recognition.

Recommendation: Additionally, to maintain a strong collaboration with private sector stakeholders, DHS may also benefit from establishing a Federal advisory committee comprised of representatives from air carriers, airports, privacy groups, and other industry partners.

With respect to implementing biometric exit at land POEs, CBP is just beginning to identify a possible technology to handle exit data collection. Like with the air environment, challenges exist regarding infrastructure and personnel. Today, most land POEs do not have the physical space required to deploy biometric technology. Furthermore, operationally, acquiring biometric data from vehicle passengers would be more difficult than doing so for those crossing on foot, because, according to CBP officials, biometric capabilities currently available would require all passengers to stop and exit their vehicle to be photographed or scanned.[98]

While CBP has said that only a small portion of non-immigrant visitors actually exit via a land POE, deploying a biometric exit program without incorporating land POEs may create a security vulnerability that could potentially be exploited. A fully-effective biometric system must be comprehensive and integrated.

V. AIR CARGO SECURITY *(Sec. 1602)*

Background:

The air cargo industry is a valuable sector of the economy; in 2016, airlines transported 52 million metric tons of goods with a global trade by value of roughly $6.8 trillion annually.[99] Three years after the 9/11 attacks, the 9/11 Commission raised alarms about the threat of a cargo-based attack, saying:

> "Concerns also remain regarding the screening and transport of checked bags and cargo. More attention and resources should be directed to reducing or mitigating the threat posed by explosives in vessels' cargo holds."[100]

[98] U.S. Customs and Border Protection, Briefing with H. Comm. on Homeland Security Majority and Minority staff (July 18, 2017).
[99] "Air Cargo," International Air Transport Association, accessed August 23, 2017, http://www.iata.org/whatwedo/cargo/Pages/index.aspx.
[100] 9/11 COMMISSION REPORT, 393.

In an effort to address this recommendation, section 1602 of the *9/11 Commission Act* required that, within three years of the date of enactment, the DHS Secretary establish a system to screen 100 percent of cargo transported on passenger aircraft in the U.S. This mandate was enacted over objections from the Transportation Security Administration (TSA) and the air cargo industry, who favored an approach whereby only high-risk cargo would be screened.[101]

On August 2, 2010, TSA announced that it met the deadline for screening 100 percent of cargo on domestic passenger flights through the implementation of the Certified Cargo Screening Program (CCSP).[102] Under this program, manufacturers, warehouses, distributors, freight forwarders, and shippers use TSA-approved technologies and procedures to screen cargo both at airports and at off-airport facilities.[103] After some delays, TSA came into full compliance with the mandate for inbound international passenger flights on December 3, 2012.[104]

On August 25, 2017, *CNN* reported that TSA, in response to a foiled Australian air-cargo-based terrorist plot, launched an examination of screening for cargo flown into and within the U.S. According to TSA, the goal of the review is to "raise the baseline on transportation security domestically and internationally and cargo security is a part of that effort."[105] Subsequently, on September 7th, TSA issued a security directive requiring enhanced screening for all cargo from Turkey, with a TSA spokesman explaining "[t]he incident in Australia just a few short weeks ago was an ominous reminder for TSA and all of our aviation partners, to include cargo carriers, that we need to continue our efforts to keep our skies secure."[106]

Findings & Recommendations:

TSA worked effectively with air cargo stakeholders to successfully implement the 100 percent screening mandate for air cargo on passenger planes. Air cargo sector stakeholders were able to adopt the required security measures without experiencing significant delays in commerce, as some had feared. Still, it is important to note that CCSP was implemented during a recession when the volume of air cargo was just 80 percent of peak volume reached

[101] Bart Elias, *Screening and Security Air Cargo: Background and Issues for Congress* (Washington DC: Congressional Research Service, 2010), 9.
[102] Transportation Security Administration, "TSA announces key milestone in cargo screening on passenger aircraft," news release, August 2, 2010, https://www.tsa.gov/news/releases/2010/08/02/tsa-announces-key-milestone-cargo-screening-passenger-aircraft.
[103] Ibid.
[104] Transportation Security Administration, "TSA sets cargo screening deadline for international inbound passenger aircraft," news release, May 16, 2012, https://www.tsa.gov/news/releases/2012/05/16/tsa-sets-cargo-screening-deadline-international-inbound-passenger-aircraft.
[105] Rene Marsh and Zachary Cohen, "TSA reviewing cargo screening, concerned about terror vulnerabilities," *CNN*, August 25, 2017, http://www.cnn.com/2017/08/25/politics/tsa-cargo-security-concerns/index.html.
[106] Rene Marsh and Sophie Tatum, "TSA will mandate air cargo from Turkey must be screened," *CNN*, September 7, 2017, http://www.cnn.com/2017/09/07/politics/tsa-air-cargo-turkey/index.html

in 2007.[107] Today, with the economy rebounding and the growth of e-commerce, the volume is closer to the 2007 peak.[108]

Currently, TSA is reportedly undertaking a review of cargo screening protocols in light of intelligence that came to light regarding terrorist efforts to place explosive device components in cargo.[109] It is important that TSA take a comprehensive look at the security protocols to ensure that they are positioned to address constantly-evolving threats.

Recommendation: As cargo volume grows, and as the nature of cargo being shipped continues to evolve as a result of the rise of e-commerce and other global economic factors, TSA should review its air cargo security policies and regulations and make any necessary updates.

Air Cargo Office

Air cargo stakeholders have raised the lack of a centralized office within TSA for air cargo security issues as a problem.[110] A dedicated air cargo office previously existed, but TSA disbanded it after the implementation of the 100 percent screening mandate. Today, cargo responsibilities are divided among multiple offices within TSA and are generally handled as part of a larger portfolio. For example, responsibility for developing and monitoring air cargo security policy rests within the Office of Security Policy and Industry Engagement, which has wide-ranging transportation security responsibilities. As long as TSA's coordination on cargo security remains disjointed, it will be difficult for TSA to accurately assess the effectiveness of cargo security screening and ensure TSA is responsive to not only the threat picture but changes in the air cargo industry.

Recommendation: Given that TSA's approach to cargo security screening is heavily reliant on effective security operations at the air cargo stakeholder level, TSA should centralize air cargo security responsibility within one office or division focused solely on air cargo security.

---

[107] U.S. Department of Transportation, Bureau of Transportation Statistics, *Air Cargo Summary Data (All): October 2002- May 2017*, accessed August 23, 2017, https://www.transtats.bts.gov/freight.asp.
[108] Ibid.
[109] *Supra*, note 106
[110] *Securing Air Cargo: Industry Perspectives*, *Hearing before Subcmte. on Transportation Protective Security*, *Comm. on Homeland Security*, *House of Representatives*, 115th Cong. (July 25, 2017) (statement of Stephen A. Alterman, President, Cargo Airline Association).

Third Party Canine Detection

More broadly, TSA should continue to work collaboratively with air cargo stakeholders to integrate innovative or new systems into existing security requirements. For some time, there has been great interest in increasing the participation of explosive detection canine teams in air cargo screening operations. Currently, only canines trained by TSA can be used to screen cargo, and since most of those canines are dedicated to passenger screening and other TSA priorities, canine resources for cargo screening are scarce. In October 2016, TSA issued a Request for Information (RFI) to solicit industry feedback to determine whether private detection canines can meet TSA detection standards. In February 2017, TSA held an Industry Day to meet with canine detection industry stakeholders.[111] TSA is currently reviewing submissions received from industry to determine next steps.

To ensure greater availability of canine screening resources, the Committee advanced legislation to authorize a process where qualified third-party canines could screen air cargo, which the *9/11 Commission Act* directed TSA to explore.[112] Section 1552 of the *DHS Authorization Act* authorizes TSA to contract with third-party vendors to train and operate explosives detection canine teams to screen air cargo to TSA standards.

Recommendation: In the event that TSA determines that third party canine teams can meet TSA screening standards for air cargo, TSA should establish a program for the utilization of third party canine resources to help air cargo stakeholders comply with the 100% screening mandate.

Air Cargo Advance Screening Program

In 2010, TSA worked with CBP to launch the Air Cargo Advance Screening (ACAS) pilot program to target air cargo shipments inbound to the U.S. and enhance air cargo supply chain security, prompted by the attempted terrorist attack in late 2010 involving two U.S.-bound packages from Yemen containing viable bombs capable of bringing down aircraft.[113] ACAS is a voluntary program under which security filing data and related information is submitted to CBP at the earliest point practicable prior to loading of the cargo but no later than four hours prior to departure of aircraft traveling to or through the U.S. CBP and TSA analyze the data to target high-risk cargo for additional screening and inspection. Since October 2012, the ACAS pilot has been extended multiple times. Most recently, CBP announced its intent to

[111] Transportation Security Administration, Request for Information- Third Party Canine Cargo Screening, (Washington DC: Federal Business Opportunities, Sol. No. HSTS02-17-I-3PK9CS) (October 21, 2016), https://www.fbo.gov/index?s=opportunity&mode=form&id=50f2434128fbdd060db4976ce0b4255b&tab=core&_cview=1.
[112] 9/11 Commission Act, 121 Stat. 395 (2007).
[113] *What Does a Secure Border Look Like?: Hearing before Subcmte. on Border and Maritime Security*, *Comm. on Homeland Security*, *House of Representatives*, 113th Cong. (February 26, 2013) (joint statement of Michael Fisher, Chief, U.S. Border Patrol, and Kevin McAleenan, Acting Assistant Commissioner, Office of Field Operations, U.S. Customs and Border Protection).

issue a notice of proposed rulemaking to incorporate ACAS as an ongoing regulatory program.[114]

Included in the *DHS Authorization Act*, which the House approved in July 2017, was a provision directing the DHS Secretary to issue a final rule to establish the ACAS program within 180 days of enactment.

Recommendation: DHS should act expeditiously to make the ACAS program permanent.

VI. SURFACE TRANSPORTATION GRANTS AND TRAINING *(Secs. 1406, 1408, 1517 and 1534)*

Background:

With security for the aviation sector hardened in response to the 9/11 attacks, terrorists view public surface transportation—such as freight and passenger trains, metros, subways, buses, and ferries—as soft targets for mass-casualty attacks. A 2012 Mineta Transportation Institute (MTI) report analyzed fifteen terrorist plots against public surface transportation that were uncovered and thwarted by law enforcement between 1997 and 2010; seven of the fifteen plots were against U.S. systems.[115] Moreover, the lethality of mass transit attacks is far higher than other types of terrorist attacks; in fact, according to MTI, public transportation attacks kill "an average of 16.3 people per device, 12.5 times more than the 1.3 people killed by the others. . . . The data also reveals that, over the long run, terrorist attacks on surface transportation targets are becoming more successful."[116]

Prospects of an escalation of such attacks in the U.S. and Western Europe are particularly concerning given the recent publication of terrorist 'how to' guide on attacking trains. On August 12, 2017, Al Qaeda in the Arabian Peninsula (AQAP) published "Train Derail Operations," a 94-page English on-line terrorism recruitment and training guide that

[114] U.S. Customs and Border Protection, Extension of the Air Cargo Advance Screening (ACAS) Pilot Program, (Washington, DC: Federal Register, 81 FR 47812) (July 22, 2016), https://www.federalregister.gov/documents/2016/07/22/2016-17366/extension-of-the-air-cargo-advance-screening-acas-pilot-program.

[115] Brian Michael Jenkins and Joseph Trella, "Carnage Interrupted: An Analysis of Fifteen Terrorist Plots Against Public Surface Transportation," *Mineta Transportation Institute*, (April 2012), http://transweb.sjsu.edu/PDFs/research/2979-analysis-of-terrorist-plots-against-public-surface-transportation.pdf.

[116] Brian Michael Jenkins and Bruce R. Butterworth, "Troubling Trends in Terrorism and Attacks on Surface Transportation: The Outlook is Grim, but People Still Have a Great Deal of Control," *Mineta Transportation Institute*, (March 2015), http://transweb.sjsu.edu/PDFs/research/terrorism-surface-transportation.pdf.

outlines how a would-be terrorist could carry out a non-martyrdom operation to derail a train in the U.S., Great Britain, or France.[117]

Transportation Security Grant Program

Addressing the security of public transit systems is challenging for the Federal government. Public transit systems are owned and operated by private stakeholders or State or local governmental entities. In order to bolster the security of such systems, section 1406 of the *9/11 Commission Act* authorized a security grant program for eligible public transportation agencies to make security improvements.[118] The Transit Security Grant Program (TSGP) competitively awards grants to transit systems to "promote sustainable, risk-based efforts to protect critical transportation infrastructure and the traveling public from acts of terrorism."[119] Grants are typically awarded to Urban Area Security Initiative (UASI) jurisdictions and, for FY17, focused on operational activities, operational packages, and capital projects including critical infrastructure vulnerability remediation.[120]

Section 1406 authorized Congress to appropriate up to $650 million in FY08, $750 million in FY09, $900 million in FY10, and $1.1 billion in FY11. Congress has never appropriated the program at the authorized level. The program's funding peak came in FY08, when it was funded at nearly $389 million.[121] In FY17, it was funded at just $88 million.[122]

Overall, TSGP has provided over $2.1 billion in security funding[123] to protect critical surface transportation and, among other things, fund transit tunnel training, canine teams, anti-terrorism teams, mobile screening teams, public awareness, and security planning.[124] TSGP's impact has been far-reaching. As such, the downward trend in grant funding is concerning.

The American Public Transportation Association (APTA) has expressed concern about the adequacy of TSGP funding to help meet the security needs of this critical sector whose ridership has surpassed 10 billion trips annually.[125] In 2016, APTA called on Congress to

---

[117] Alexandra Ma, "Al Qaeda publishes an entire magazine on how to derail trains in Europe and America," *Business Insider*, August 16, 2017, http://www.businessinsider.com/al-qaeda-published-18-page-guide-on-how-to-derail-trains-in-europe-and-america-2017-8?r=UK&IR=T.

[118] Funding for this grant program was $150 million in FY05, the first year of the program.

[119] U.S. Department of Homeland Security, Fiscal Year 2017 Transit Security Grant Program, accessed August 23, 2017, 1, https://www.fema.gov/media-library-data/1496325850639-1b82069b2a3c2619512cc7d88e4be8d6/FY_2017_TSGP_Fact_Sheet_FINAL_508.pdf

[120] Ibid.

[121] Federal Emergency Management Agency, U.S. Department of Homeland Security, *FY08 Transit Security Grant Program*; (2008). https://www.fema.gov/fy-2008-transit-security-grant-program.

[122] *Supra*, note 119.

[123] Christopher T. McKay, Modal Manager, Transit, Surface Division, Transportation Security Administration, "Surface Transportation Landscape Mass Transit Passenger Rail" (PowerPoint presentation, U.S. Department of Transportation, Washington, DC, April 24, 2017), 8, https://www.transit.dot.gov/sites/fta.dot.gov/files/docs/regulations-and-guidance/safety/60591/surface-transportation-landscape-mass-transit-and-passenger-rail.pdf

[124] Ibid.

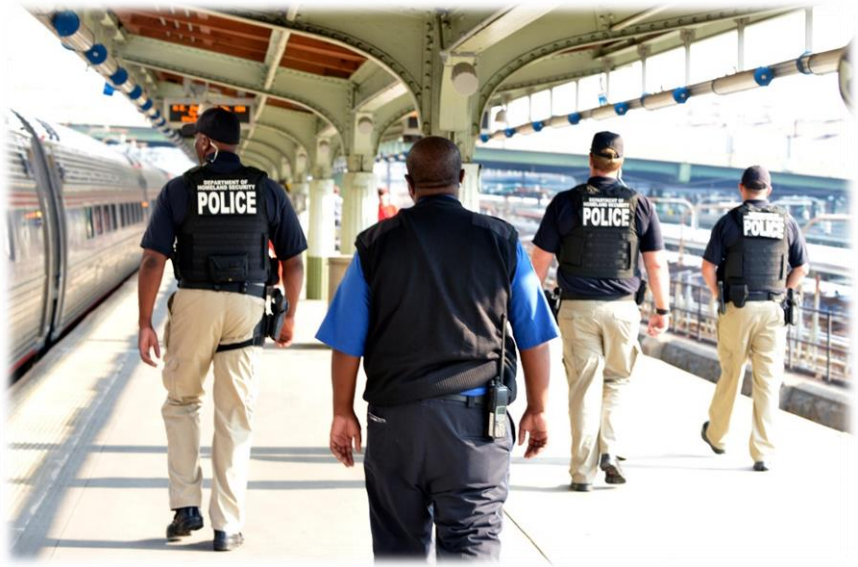
[125] *On Transit and Rail Security Grants, the FEMA State and Local Grant Program, and TSA Surface Transportation Security, within the Fiscal Year 2017 Appropriations for the Department of Homeland Security, testimony submitted to Subcmte. on Homeland Security, Comm. on Appropriations, Senate*, 114th Cong. (April 1, 2016) (statement of Michael P. Melaniphy, President and CEO, American Public Transportation Association), http://www.apta.com/gap/testimony/2016/Documents/160401_SenateTestimony.pdf.

restore TSGP funding "to levels closer to those authorized under the 9/11 Commission Act," explaining that transit agencies have more than $6 billion of capital and operational security needs and that, despite significant spending on security by State and local government, "TSGP is the primary source of Federal funding for security needs of public transportation agencies."[126]

During the House Homeland Security Committee's consideration of the *DHS Authorization Act*, Vice Ranking Member Bonnie Watson Coleman (D-NJ) offered an amendment that would have authorized TSGP at $400 million. This amendment was rejected, however, the underlying bill raises the TSGP authorization level to $200 million.

Frontline Training

Incidents in recent years serve as stark reminders that terrorists are willing to exploit surface transportation security vulnerabilities to carry out attacks. For example, in 2008, an individual was arrested for sharing details of the Long Island Railroad with al Qaeda in an effort to help bomb New York City's Penn Station.[127] In September 2009, three individuals were arrested for planning to detonate backpack bombs at Grand Central Station and Times Square.[128] And in 2015, a terrorist opened fire on a train bound for Paris, but through the selfless acts of passengers, the attacker was subdued before being able to successfully carry out his attack.[129] These incidents highlight the need for formal, cohesive training for public transportation employees.



The *9/11 Commission Act* recognized that the Department had a role to play in bolstering preparedness in surface transportation systems. Section 1408(a) required that within one year, the DHS Secretary develop and issue detailed final regulations for a public transportation security training program to prepare public transportation

[126] Ibid.
[127] Paul Cruickshank, "Al Qaeda's 2008 plan to hit Long Island Railroad revealed," Security Clearance *CNN*, April 23, 2012, http://security.blogs.cnn.com/2012/04/23/al-qaedas-2008-plan-to-hit-long-island-railroad-revealed/.
[128] Susan Candiotti, "Source: Terror plot targeting Times Square, Grand Central stations," *CNN*, April 12, 2010, http://www.cnn.com/2010/CRIME/04/12/new.york.plot/index.html.
[129] Michael Birnbaum, "A Change of Seats for 3 Americans Led to Saved Lives on Paris-bound Train," *Washington Post*, August 24, 2015, https://www.washingtonpost.com/world/as-french-train-suspect-is-interrogated-questions-mount-on-europes-security/2015/08/23/088ff2fe-4923-11e5-9f53-d1e3ddfd0cda_story.html?utm_term=.19d76a7f6042.

employees, including frontline employees, for potential security threats and conditions. Similarly, sections 1517(a) and 1534(a) required that within six months, the DHS Secretary develop and issue detailed final regulations for railroad and over-the-road bus frontline employees, respectively, to receive baseline training to address security threats and conditions.

In the *2014 National Strategy for Transportation Security*, TSA listed "security training" as one of seven risk-based priorities for surface transportation.[130] Roughly twenty months later, on December 16, 2016, TSA published a proposed in the Federal Register "to solidify the enhanced baseline of security for higher-risk surface transportation operations by improving and sustaining the capability of employees to observe, assess, and respond to security risks and potential security breaches."[131] The proposed rule would require public transportation operators[132] to submit proposed security training programs to TSA for review and approval, but TSA would not set standards, such as requiring that workers in such programs pass tests or demonstrate particular skills. With respect to the timeline for the provision of approved training, the proposed rule acknowledges that the *9/11 Commission Act* requires initial public transportation training within one year of program approval, and railroad and over-the-road bus training within six months of approval, but in response to stakeholder concerns, proposes that extensions be allowed upon a showing of good cause.[133] By March 16, 2017, the date that the comment period closed, TSA had received 30 comments from a wide range of stakeholders.[134] Surface transportation stakeholders have raised concerns with the proposed rule related to potential costs of training employees, maintaining training records, training compliance inspections, and assigning security personnel and reporting incidents to TSA.[135]

Findings & Recommendations:

In the ten years since enactment of the *9/11 Commission Act*, TSA has made little progress in requiring that frontline transportation security workers receive critical baseline security training. Though a proposed rule was published last December, prospects for further action by the Trump Administration are unclear, particularly given that no funding was requested in the Administration's FY18 budget request to implement a final rule.

[130] Department of Homeland Security, *2014 National Strategy for Transportation Security: Report to Congress*, (Washington, DC: April 17, 2015). The seven risk-based priorities are: security planning, security training, security exercises, intelligence and security information sharing, risk reduction, community outreach, and critical infrastructure protection; Transportation Security Administration,

[131] Transportation Security Administration, Department of Homeland Security, Security Training for Surface Transportation Employees, (Washington, DC: Federal Register, 81 FR 91336) (December 16, 2016), https://www.gpo.gov/fdsys/pkg/FR-2016-12-16/pdf/2016-28298.pdf.

[132] Public transportation operators are defined as freight railroad carriers, public transportation agencies (including rail mass transit and bus systems), passenger railroad carriers, and over-the-road bus companies.

[133] Security Training for Surface Transportation Employees, (2016)(81 FR 91336, 91387).

[134] Ibid.

[135] Ibid.

Recommendations: TSA should act expeditiously to finalize a rule that is responsive to comments and designed to ensure maximum compliance and minimum burdens on these critical infrastructure operators. The *9/11 Commission Act* required initial and recurrent training; TSA should aggressively engage with surface transportation stakeholders, including organizations that represent frontline workers, about opportunities for more advanced training and exercises.

Without decisive action, training of public transportation employees will continue to be at the discretion of surface transportation stakeholders and, as such, the Federal government will be unable to gauge preparedness for terror attacks across public, freight rail, and bus transportation systems.

The 2004 commuter train attacks in Madrid, 2005 London tube bombings, and 2016 metro station attacks in Brussels underscore that bustling surface transportation hubs are attractive terrorist targets. At its height, TSGP was funded at $388 million. In FY17, only $88 million was dedicated to TSGP. Today, the gains achieved over the past decade at enhancing the security of the systems on which Americans rely to live and work are at stake. Funding for TSGP must be increased.

Recommendation: Congress should, at a minimum, fund the TSGP at $200 million annually, the level authorized in H.R. 2825, the *DHS Authorization Act of 2017* and immediately consider a path to full funding restoration.

VII. MARITIME CARGO SECURITY *(Sec. 1701)*

Background:

The 9/11 Commission identified a "failure of imagination" within our Federal government as contributing to the 9/11 attacks. As explained by Lee Hamilton, the Commission's Vice Chairman,

> [t]here were hints here and there in a variety of places, but as a whole the government didn't grasp the potential scenario that occurred.... [W]e have to understand we're contending here against a very entrepreneurial, very innovative enemy who know how to penetrate our open society. They understood that they could get a four-inch knife on board, but maybe not a six-inch knife…. So we have to have an imagination strong enough to think about

a number of different scenarios, and it is a very key part of a counterterrorism strategy.[136]

In 2003, a report commissioned by the U.S. Department of Transportation estimated that the economic impact of a nuclear terrorist attack on a major U.S. seaport "would create disruption of U.S. trade valued at $100-200 billion, property damage of $50-500 billion, and 50,000 to 1,000,000 lives. . . lost."[137]

Within the Federal government, CBP is the primary agency responsible for screening, monitoring, inspecting, and facilitating cargo at U.S. POEs. According to CBP, every year, more than 11 million maritime containers arrive at our seaports.[138] Today, statutory and regulatory requirements for the submission of cargo manifest data and the development of targeting capabilities at the National Targeting Center (NTC) provide CBP with the ability to detect potential threats before a vessel or shipment arrives in the U.S.[139]

In 2006, DHS was directed, once certain conditions were met, to work with the Department of Energy and foreign partners to ensure that, "as soon as possible," all U.S.-bound containers were scanned, through an integrated non-intrusive inspection (NII) and radiation detection system, before arriving in the U.S.[140] The following year, section 1701 of the *9/11 Commission Act* amended that law to require that no later than July 1, 2012, the DHS Secretary complete full-scale implementation of the integrated scanning system and prohibit any U.S.-bound container from entering a U.S.-port unless it has undergone scanning through the system at a foreign port. Under the law, the DHS Secretary is permitted to extend the deadline for two years at one or more ports, if the Secretary certifies that at least two of the six conditions exist.[141]

---

[136] Lee Hamilton, Vice Chairman, 9/11 Commission, interview by Fredricka Whitfield, *CNN*, July 22, 2004, http://edition.cnn.com/TRANSCRIPTS/0407/22/se.02.html

[137] Clark C. Abt, "The Economic Impact of Nuclear Terrorist Attacks on Freight Transport Systems in an Age of Seaport Vulnerability," Abt Associates Inc. (prepared for U.S. Department of Transportation) (April 30, 2003), 7, http://www.abtassociates.com/reports/ES-Economic_Impact_of_Nuclear_Terrorist_Attacks.pdf

[138] *An Examination of the Maritime Nuclear Smuggling Threat and Other Port Security and Smuggling Risks in the U.S.: Hearing before Subcmte on Border and Maritime Security, Comm. on Homeland Security, House of Representatives*, 114th Cong. (July 7, 2016) (statement Todd C. Owen, Executive Assistant Commissioner, Office of Field Operations, U.S. Customs and Border Protection).

[139] Ibid.

[140] Section 232(b) of the Security and Accountability for Every Port Act (SAFE Port Act) of 2006, Pub. L. No. 109-347, 120 Stat. 1916 (2006).

[141] The conditions for an extension at one or more ports are that scanning systems are not available for purchase and installation; systems do not have a sufficiently low false alarm rate; systems cannot be purchased, deployed, or operated at overseas ports;

100% Scanning Mandate Deadline

Since 2012, successive DHS Secretaries have extended the 100 percent scanning deadline, as permitted in section 1701. As such, the statutory deadline has been extended three times, with the last extension anticipated to expire in July 2018.

- On May 2, 2012, then-Secretary Janet Napolitano notified Congress that she would extend the deadline for two years.[142] In the notification, Secretary Napolitano certified that the use of systems to scan containers would have significant and negative impact on trade capacity and cargo flows and that systems to scan containers could not be purchased, deployed, or operated at overseas ports due to limited physical infrastructure.[143]

- On May 5, 2014, then-DHS Secretary Jeh Johnson notified Congress that the deadline would be extended for an additional two years given that the conditions cited in 2012 had not changed substantially.[144] However, in his notification, Secretary Johnson mentioned that DHS was making "good faith" efforts to comply with the mandate; improved targeting; engagement with private sector stakeholders and international partners; and efforts to address other potential vulnerabilities through a broad, multi-faceted, and risk-based approach.[145]

- On May 2, 2016, then-Secretary Johnson notified Congress of the Department's third deadline extension for the 100 percent scanning requirement.[146] Though the letter cited many of the same previous reasons for the extension, it referenced that progress toward meeting the mandate now included CSI operations in three additional foreign ports and improved targeting capabilities and models.

Concurrent with the 2016 extension notification, DHS issued an RFI to solicit "strategies to improve maritime supply chain security and achieve 100 percent overseas scanning."[147] Through this RFI, DHS sought input for new programs, capabilities, models, strategies, or approaches, through which DHS and its partners could make progress toward achieving the 100 percent scanning requirement and enhance the security of U.S.-bound maritime cargo. DHS sought both technical and non-technical approaches from a broad range of responders,

---

systems cannot be integrated with existing systems; and use of systems will significantly impact trade capacity and the flow of cargo.

[142] Janet Napolitano, Secretary of Homeland Security, Letter to Congress, May 2, 2012.

[143] Office of Policy, *U.S. Department of Homeland Security*, *Scanning of Maritime Cargo Containers: Fiscal Year 2016 Report to Congress* (Washington, DC: May 2, 2016), 3.

[144] Jeh Johnson, Secretary of Homeland Security, Letter to Congress, May 5, 2014.

[145] Ibid.

[146] Jeh Johnson, Secretary of Homeland Security, Letter to Congress, May 2, 2016.

[147] Department of Homeland Security, Request for Information, Strategies to Improve Maritime Supply Chain Security and Achieve 100% Overseas Scanning, (Washington, DC: Federal Business Opportunities, Sol. No. DHS100Scanning) (May 2, 2016), https://www.fbo.gov/index?s=opportunity&mode=form&tab=core&id=5b3a3915390f012eb21ead100c816eb1&_cview=0.

including providers of supplies and services, non-vendor stakeholders, and non-traditional contractors.[148]

DHS received 25 submissions to the RFI from a variety of sources including industry, terminal operators, vendors, and academia.[149] According to Department officials, responses were evaluated based on eight criteria that moved DHS closer to increasing the amount of U.S.-bound maritime cargo scanned, improving global radiological and nuclear detection capability and capacity, and reducing the amount of nuclear and other radioactive materials out of regulatory control in the global maritime shipping environment.[150]

On July 11, 2017, then-DHS Secretary Kelly notified Congress that an additional extension to the deadline would be required in 2018 as the RFI process did not result in DHS identifying a strategy or approach that would allow the Department to meet "full-scale implementation of 100 percent scanning."[151] However, certain submissions were found promising in improving overall supply chain security, and two of these proposals would be piloted.[152]

Layered, Risk-Based Approach

The Department's current approach to screening maritime cargo involves: (1) requiring carriers and importers to submit information about shipments in advance of their departure from a foreign port for a U.S. port of entry; (2) "targeting" or identifying shipments that pose a higher risk based on analysis of submitted information from other law enforcement and intelligence holdings; and (3) requiring that high-risk cargo be scanned and/or physically inspected at the foreign port, prior to departure for the U.S., to mitigate potential risks.[153] As part of this process, DHS has formed public-private partnerships in which shippers voluntarily add security measures to their existing process, and partnerships with foreign governments, where the U.S. and the other country "mutually recognize" the equivalency of each other's cargo security regimes.[154]

DHS officials have testified that it gets manifest data on nearly all U.S.-bound cargo and that nearly all arriving cargo goes through radiation portal monitors at a U.S. seaport but that only five percent of such cargo is actually scanned overseas.[155] As for inbound cargo deemed high-risk by CBP, just 85 percent is inspected overseas.[156]

---

[148] U.S. Department of Homeland Security, Briefing with H. Comm. on Homeland Security Majority and Minority staff (August 10, 2016, November 15, 2016, and July 12, 2017).
[149] Ibid.
[150] *Supra*, note 147.
[151] John F. Kelly, Secretary of Homeland Security, Letter to Congress, July 11, 2017.
[152] Ibid.
[153] Vivian C. Jones and Lisa N. Sacco, *U.S. Customs and Border Protection Trade Facilitation, Enforcement, and Security* (CRS Report No. R43014) (Washington, DC: Congressional Research Service, 2015)
[154] Ibid.
[155] *Balancing Maritime Security and Trade Facilitation: Protecting Our Ports, Increasing Commerce and Securing the Supply Chain- Part I: Hearing before Subcmte. on Border and Maritime Security, Comm. on Homeland Security, House of Representatives*, 112th Cong. (February 7, 2012) (statement of David Heyman, Assistant Secretary, Office of Policy, U.S. Department of Homeland Security).
[156] *Evaluating Port Security: Progress Made and Challenges Ahead: Hearing before Comm. on Homeland Security and Governmental Affairs, Senate*, 113th Cong. (June 4, 2014) (statement of Kevin K. McAleenan, Acting Deputy Commissioner, U.S. Customs and Border Protection).

Scanning Conducted Abroad

CBP's two major programs for overseas maritime cargo screening are the Container Security Initiative (CSI) and the Secure Freight Initiative (SFI). CSI is a bilateral government partnership program operated by CBP that aims to identify and examine U.S.-bound cargo container shipments that are at risk of containing weapons of mass destruction or other terrorist contraband. As part of the program, CBP officers are stationed at certain foreign seaports to review information about U.S.-bound containerized cargo shipments. CBP evaluates the risk of U.S.-bound container shipments and requests examinations of high-risk container shipments before they are loaded onto vessels.[157]

The CSI program began as a pilot in 2002 and was made permanent in 2006.[158] Currently, CSI is operational at 60 ports in North America, Europe, Asia, Africa, the Middle East, and Latin and Central America. CBP estimates that, through the CSI program, it prescreens over 80 percent of all maritime containerized cargo imported into the U.S. CBP uses its CSI Port Risk Matrix, Port Priority Map, and other tools available through CSI, to assess whether changes need to be made to CSI ports worldwide.[159] According to GAO, by developing and employing these risk-assessment tools, CBP is better positioned to ensure that resources are allocated to best mitigate the risk of importing nuclear devices or other terrorist contraband into the U.S. through the supply chain.[160]

In response to a 2006 requirement that U.S.-bound cargo containers be scanned overseas, CBP established SFI at six overseas ports.[161] Through this program, radiation detection and NII equipment is used to scan cargo containers before they are loaded onto U.S.-bound vessels.[162] Today, SFI is operational in Qasim, Pakistan and the Port of Aqaba in Jordan.[163]

<u>Findings & Recommendations:</u>

---

[157] *An Examination of the Maritime Nuclear Smuggling Threat and Other Port Security and Smuggling Risks in the U.S.: Hearing before Subcmte. on Border and Maritime Security, Comm. on Homeland Security, House of Representatives*, 114th Cong. (July 7, 2016) (statement Jennifer Grover, Director, Homeland Security and Justice, U.S. Government Accountability Office).

[158] Section 205 of the Security and Accountability for Every Port Act (SAFE Port Act) of 2006 (P.L. 109-347), October 13, 2006.

[159] *Supra*, note 138.

[160] *Supra*, note 157.

[161] *Supply Chain Security: CBP Works with International Entities to Promote Global Customs Security Standards and Initiatives, but Challenges Remain* (GAO-08-538) (Washington, D.C.: U.S Government Accountability Office, 2008). Under the program, in 2008, all containers were scanned at three seaports (Qasim, Pakistan; Puerto Cortez, Honduras; and Southampton, UK) and containers were scanned on a more limited basis at three seaports (Hong Kong; Busan, South Korea; and Salalah, Oman).

[162] *Supra*, note 157.

[163] *Supra*, note 138.

Over the past decade, the Department has made little progress at ensuring that all U.S.-bound maritime cargo is scanned overseas. Instead, it has fallen into a pattern of issuing extension after extension to push out the statutory deadline. A decade ago, when the law was enacted, Congress understood that full implementation of section 1701 was going to be a considerable challenge. That is why Congress included a provision allowing for the DHS Secretary to execute extensions, as necessary. However, it is troubling that DHS has repeatedly extended the deadline in a blanket manner, without any specificity on what obstacles were encountered at each overseas port.

Recommendation: Congress should amend the law to require that before the DHS Secretary can exercise extension authority, overseas port assessments be completed that inform any certification about obstacles to implementation.

As noted above, in July 2017, then-Secretary Kelly expressed the Department's commitment to achieving full compliance with the mandate. This expression of support for the law builds upon efforts by the prior DHS Secretary—Secretary Johnson—to reengage with the maritime security community on the mandate, with the issuance of the 2016 RFI.

Today, two pilots are underway including an integrated scanning system at the Port of Boston and a Common Viewer System for sharing x-ray data at Norfolk and Savannah.[164] These pilots are, at least in part, informed by the results of the RFI but ten years after enactment of the *9/11 Commission Act*, DHS still lacks an operational scheme or plan for achieving the mandate. Without a plan to move toward incremental achievement of the mandate, prospects for achieving full implementation are dubious.

That said, recent enhancements to the NTC's nuclear threat targeting capabilities provide greater confidence about the accuracy of CBP's determinations that certain containers are high-risk. Previously, DHS has said that just five percent of cargo gets scanned overseas. In 2014, Department officials testified that within the subset of cargo that CBP deems as high risk, just 85 percent gets inspected overseas but that it was working "to increase the percentage of containers scanned abroad, with an emphasis on high-risk cargo, by prioritizing diplomatic engagement with host governments to increase their support of

[164] Letter from John F. Kelly, Secretary of Homeland Security to Congress, July 11, 2017.

current Container Security Initiative operations and discuss potential expansion to additional key ports."[165]

Recommendation: DHS should develop and execute a strategy of engagement with international partners to put protocols in place to ensure that, at a minimum, all cargo it deems as at a high-risk for containing radiological and nuclear material is scanned before arriving at a U.S. port.

Recommendation: Once 100% high-risk cargo scanning protocols are in place, the Department should seek to leverage efforts at closing the "high-risk" cargo security gap to improve broader efforts at implementing the broader 100% scanning mandate.

VIII. SURFACE TRANSPORTATION SECURITY PROGRAMS *(Secs. 1303, 1304, 1404, 1405, 1512, and 1531)*

Background:

The surface transportation sector is one of the most important lifelines of our nation's economy. According to testimony from a TSA official, there are more than 500 freight railroads operating on 140,000 miles of track, more than eight million commercial trucks and nearly 4,000 commercial bus companies traveling on four million miles of roadway.[166] Annually, bus companies carry 750 million passengers intercity and approximately 10 billion trips are made on rail transit.[167] With so many people utilizing surface transportation, the need for strong leadership from TSA in surface transportation security cannot be overstated.

[165] *Evaluating Port Security: Progress Made and Challenges Ahead, Hearing before Comm. on Homeland Security and Governmental Affairs, Senate*, 113th Cong. (June 4, 2014) (joint testimony of Ellen McClain, Deputy Assistant Secretary for Transborder Policy, DHS Office of Policy, RDML Paul Thomas, U.S. Coast Guard, Kevin K. McAleenan, Acting Deputy Commissioner, U.S. Customs and Border Protection, Steve Sadler, Assistant Administrator, DHS Office of Intelligence and Analysis, Brian E. Kamoie, Assistant Administrator for Grant Programs, Federal Emergency Management Agency, U.S. Department of Homeland Security).

[166] *Safeguarding Our Nation's Surface Transportation Systems Against Evolving Terrorist Threats: Hearing before Subcmtes. on Transportation Security and Counterterrorism and Intelligence, Comm. on Homeland Security, House of Representatives*, 114th Cong. (September 17, 2015) (Eddie Mayenschein, Assistant Administrator, Office of Security Policy and Industry Engagement, Transportation Security Administration).

[167] Ibid.

The *9/11 Commission Act* included a number of provisions targeted at enhancing surface transportation. In addition to TSGP and the frontline transportation workers' training requirements (as discussed starting on page 37), the *9/11 Commission Act* directed the following specific actions to enhance surface transportation security:

- Visible Intermodal Protection and Response (VIPR) teams (section 1303);
- surface transportation security inspectors by TSA to assist in efforts to enhance security against terrorism and other threats and to enforce applicable security regulations and directives (section 1304);
- a National Strategy for Public Transportation Security (section 1404); and
- security assessments of public transportation (section 1405), railroad (section 1512) and over-the-road bus (section 1531) systems, DHS Secretarial determinations as to which systems are at a high risk for terrorism, and comprehensive security plans for such systems.

Taken together, these provisions were intended to significantly enhance Federal surface transportation security efforts.

Visible Intermodal Protection and Response (VIPR) teams

In 2008, TSA launched the VIPR team program. VIPR teams consist of Federal Air Marshals, Transportation Security Specialists-Explosives, Transportation Security Inspectors, canine units, and State and local law enforcement partners, and, at the request of a transportation security stakeholder, conduct operations in airports and major transportation hubs to deter and detect suspicious activity. Today, the VIPR program is arguably TSA's most prominent surface transportation program.

In FY08, TSA received $20 million to establish 10 VIPR teams. In FY10, an additional $25 million was provided to TSA to stand up 15 more teams across the country. In FY12, TSA received funding to add 12 teams to bring the total to 37 VIPR teams.[168] In 2012, the Department's Office of Inspector General (OIG) issued a report citing a number of organizational, programmatic, and operational challenges that hinder the program and 16 recommendations for action by TSA.[169] Subsequently, funding for expanding VIPR stagnated and, in FY18, the Trump Administration proposed reducing the program's budget by $43 million, which would force the program to shrink to just eight teams.

[168] *Efficiency and Effectiveness of TSA's Visible Intermodal Prevention and Response Program Within Rail and Mass Transit Systems* (OIG-12-103). Washington, DC: Office of Inspector General, U.S. Department of Homeland Security, 2012.
[169] Ibid.

During the House Homeland Security Committee's consideration of H.R. 2825, the *DHS Authorization Act*, Vice Ranking Member Bonnie Watson Coleman (D-NJ) offered an amendment that would authorize TSA to maintain 30 VIPR teams. The amendment was accepted in H.R. 2825, which the House approved on July 20, 2017.

Surface Transportation Inspectors

Currently, TSA deploys roughly 260 surface transportation security inspectors[170] in 49 field offices[171] to ensure and regulate compliance within the cargo supply chain and to perform security inspections across all modes of transportation. Over the years, the number of inspectors has fluctuated. In FY08, there were 175 inspectors and in FY11 there were 404.[172] The number of surface inspectors decreased to 260 in FY16.[173]

In 2009, it came to light that TSA was struggling to balance aviation and surface responsibilities for the surface inspectors and that TSA had not completed a workforce plan for the program.[174] In 2014, the Government Accountability Office (GAO) found that a lack of guidance for TSA's surface inspectors created inconsistent reporting of rail security incidents and that TSA had not consistently enforced the requirement that rail agencies report security incidents, which resulted in poor data on the number and types of incidents. GAO reported that TSA was lacking a systematic process for gathering and addressing comments from surface transportation stakeholders regarding the effectiveness of its information-sharing efforts.[175] In 2015, GAO testified that TSA had taken steps to address the program's challenges that included the distribution of guidance regarding reporting requirements to the field, reforms to improve the consistency of its inspection process, and improvements to how TSA captures data on previously unreported security incidents.[176]

---

[170] *Protecting Our Passengers: Perspectives on Securing Surface Transportation in New Jersey and New York*, *Hearing before Subcmte. on Transportation Protective Security*, *Comm. on Homeland Security*, *House of Representatives*, 114th Cong. (June 21, 2016) (statement of Sonya Proctor, Director, Surface Division, Office of Security Policy and Industry Engagement, Transportation Security Administration).

[171] *TSA Has Taken Steps Designed to Develop Processes for Sharing and Analyzing Information and to Improve Rail Security Incident Reporting* (GAO-15-205T). Washington, DC: U.S. Government Accountability Office, 2015.

[172] Bart Elias, David Randall Peterman, John Frittelli, *Transportation Security: Issues for the 114th Congress* (CRS Report No. RL33512) (Washington, DC: Congressional Research Service, 2016), 16.

[173] *Supra*, note 170.

[174] *Transportation Security: Key Actions Have Been Taken to Enhance Mass Transit and Passenger Rail Security, but Opportunities Exist to Strengthen Federal Strategy and Programs* (GAO-09-678). Washington, DC: U.S. Government Accountability Office, 2009, 50.

[175] *Supra*, note 171.

[176] *Safeguarding Our Nation's Surface Transportation Systems Against Evolving Terrorist Threats: Hearing before Subcmtes. on Transportation Security and Counterterrorism and Intelligence, H. Comm. on Homeland Security, House of Representatives*,

Presently, GAO is performing a review of the surface transportation inspectors. In their preliminary conversations with staff, GAO has indicated that for fiscal years 2013 through March 2017, approximately 80 percent of the surface inspectors' work was spent on voluntary non-regulatory duties determined largely by local management. GAO has told Committee staff that from fiscal years 2013 through 2016, most of TSA's surface regulatory inspections and 35 percent to 45 percent of surface inspectors' time overall was spent on the lowest risk surface transportation mode as determined by TSA risk assessments.[177]

National Strategy for Public Transportation Security

In 2010, TSA issued the Mass Transit Modal Annex to the Transportation System-Sector Specific Plan that set forth the Federal government's strategic objectives with respect to security public transportation and stated that the annex fulfilled section 1404 of the *9/11 Commission Act.*[178] TSA also issued in 2010 the *Surface Transportation Priority Assessment*, which set forth 20 recommendations providing "a comprehensive framework for the continued improvement of surface transportation security."[179] Section 1404 required the DHS Secretary to develop and implement a modal plan for public transportation security, entitled the "National Strategy for Public Transportation Security." The purpose of the plan is to establish guidelines for public transportation entities that minimize security threats and maximize the ability of public transportation systems to mitigate damage resulting from a terrorist attack or other major incident. Section 1404 allowed for combining this strategy with comprehensive critical infrastructure strategic planning, as was done in 2010.

Vulnerability Assessments and Security Plans

In an effort to enhance the security of surface transportation systems—public transportation, railroad, and over-the-road bus systems—at high risk for terrorism, sections 1405, 1512, and 1531 of the *9/11 Commission Act* required vulnerability assessments to be completed and, for those systems determined by the DHS Secretary as being high-risk, security plans to be developed and implemented. To carry out the provisions, DHS was required to undertake the notice and comment process with surface transportation stakeholders. Over the past decade, TSA has not published the required regulations. According to a May 2016 DHS OIG report, "TSA attributes the delays in implementing the…requirements from the *9/11 Act* primarily to the complex Federal rulemaking process.

114th Cong. (September 17, 2015) (Jennifer Grover, Director, Homeland Security and Justice, U.S. Government Accountability Office).

[177] U.S. Government Accountability Office, Briefing with H. Comm. on Homeland Security Majority and Minority staff (June 19, 2017).

[178] U.S. Department of Homeland Security, *Transportation Systems Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan* (Washington DC: 2010), 215, https://www.dhs.gov/sites/default/files/publications/nipp-ssp-transportation-systems-2010-508.pdf.

[179] Transportation Security Administration, U.S. Department of Homeland Security, *Surface Transportation Priority Assessment*; (2010) https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/STSA.pdf.

Although the rulemaking process can be lengthy, TSA has not prioritized the need to implement these…requirements."[180]

On December 16, 2016, TSA published an advance notice of proposed rulemaking on Surface Transportation Vulnerability Assessments and Security Plans with the goal of establishing a "uniform base of vulnerability assessments and security plans for security systems and operations, as well as critical assets and/or infrastructure that these owner/operators may own or control."[181] While the notice represents the biggest step TSA has taken in implementing these provisions, the timeline for full implementation is unclear.

In the absence of regulations, TSA has established programs and initiatives for the assessment of public transportation system security and voluntary security measures for such systems. For example, in 2006 TSA created the Baseline Assessment for Security Enhancement (BASE) program, through which Surface Transportation Security Inspectors conduct assessments of mass transit and passenger rail agencies and over-the-road bus operators, and help such systems develop plans to remediate identified vulnerabilities.[182] Additionally, TSA completed a national threat assessment for transit and passenger rail in 2010, and in 2011 DHS established security objectives in the Transportation System Sector-Specific Plan. TSA reports that agencies and stakeholders have voluntarily implemented security measures that meet the spirit of many of the *9/11 Commission Act* requirements, but full implementation will not occur until regulations are published.[183]

Findings & Recommendations:

As the 9/11 Commission noted, the nation's surface transportation systems "such as railroads and mass transit systems are hard to protect because they are so accessible and extensive."[184] As more cities look to build and expand their public transportation infrastructure, it is important that the Administration and Congress focus on how to effectively partner with State and local jurisdictions in securing public transportation— these systems transport millions of Americans every day.

[180] *TSA Oversight of National Passenger Rail System Security* (OIG-16-91). Washington, DC: Office of Inspector General, U.S. Department of Homeland Security, 2016.
[181] Transportation Security Administration, Department of Homeland Security, Surface Transportation Vulnerability Assessments and Security Plans, (Washington, DC: Federal Register, 81 FR 91401, 91403) (December 16, 2016), https://www.gpo.gov/fdsys/pkg/FR-2016-12-16/pdf/2016-28300.pdf
[182] Ibid.
[183] *Supra*, note 170.
[184] 9/11 COMMISSION REPORT, 391.

Presently, surface security accounts for roughly two percent of TSA's budget. Arguably, the most prominent TSA surface transportation program is the VIPR program. The Administration's FY18 budget proposal would eviscerate it and offers nothing to fill the breach.

Recommendation: Congress should reject the Trump Administration's proposal to cut VIPR funding by $43 million and, at the same time, demand that TSA enhance the program as recommended by DHS OIG to ensure that the program can address the ever-evolving threat landscape, including by establishing metrics to measure the program's efficacy.

Committee Democrats have been consistent in their support of the VIPR teams and succeeded in having language included in the *DHS Authorization Act of 2017* to ensure that VIPR teams are not reduced, as the Administration's FY18 Budget proposes.

Another key TSA resource for surface transportation is the cadre of inspectors. It is critical that TSA continue to address GAO recommendations to improve operations and, like with the VIPR program, develop metrics to ensure that Congress and the American people can accurately assess the contributions of this program to the nation's security.

Finally, with respect to the mandate that DHS issue a rulemaking for vulnerability assessments for at-risk surface transportation systems and security plans for high-risk systems, it is long overdue for DHS and the stakeholder community to come together to put mandatory baseline security performance standards in place. DHS should consider the lessons learned by another DHS security program, the Chemical Facility Anti-Terrorism Standards program, which utilizes a similar approach to protecting critical infrastructure.

Recommendation: TSA should issue, by the end of the year, a proposed rule that takes into account stakeholder feedback received to the ANPRM and reflects lessons learned by the Department's National Protection and Programs Directorate about how to establish a vulnerability assessment and security plan program.

IX. QUADRENNIAL HOMELAND SECURITY REVIEW *(Sec. 2401)*

Background:

DHS was established in response to the 9/11 attacks by combining 22 existing Federal agencies, with a goal of preventing terrorist attacks, creating a strengthened homeland security enterprise (HSE), and enhancing the Nation's preparedness, response, and resilience to homeland security threats. Over the past 15 years, the Department's missions have expanded far beyond border security along the air, land, and sea borders and emergency response and recovery, to bolstering cybersecurity and countering violent extremism. As the third-largest Federal department, and with such diverse responsibilities, it is essential that the Department's priorities, programs, and structure evolve so that DHS can effectively confront existing and emerging threats and challenges.

To ensure that the Department undertakes strategic prioritization and organizational reviews on a regular basis, section 2401 of the *9/11 Commission Act* directs DHS to produce, every four years, a unified, strategic framework for homeland security missions and goals, known as the Quadrennial Homeland Security Review (QHSR).

Modeled in part after the Department of Defense's Quadrennial Defense Review, the QHSR requirement is intended to ensure that DHS' priorities, programs, and structure are informed by a comprehensive assessment that includes (1) a description of the threats to the assumed or defined national homeland security interests; (2) the national homeland security strategy, including a prioritized list of the United States' critical homeland security missions; (3) an assessment of the organizational alignment of DHS with the applicable national homeland security strategy and the homeland security mission areas outlined; and (4) a discussion of the status of cooperation among Federal agencies in the effort to promote national homeland security, among other elements. A key feature of the QHSR is a focus on strengthening and maturing the HSE— the Federal, State, local, tribal, territorial, nongovernmental, and private-sector entities, as well as individuals, families, and communities who share a common national interest in the safety and security of America and the American population.[185]

The first QHSR was completed in 2010, and was produced to "outline the strategic framework to guide the activities of participants in homeland security toward a common end".[186] This initial QHSR identified five homeland security missions—(1) preventing terrorism and enhancing security; (2) securing and managing our borders; (3) enforcing and administering our immigration laws; (4) safeguarding and securing cyberspace; and (5) ensuring resilience to disasters—and goals and objectives to be achieved within each mission.[187]

[185] 9/11 Commission Act, 121 Stat. 544 (2007).
[186] U.S. Department of Homeland Security, Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland (Washington, DC: February 2010), vi, https://www.dhs.gov/xlibrary/assets/qhsr_report.pdf.
[187] Ibid.

GAO reviewed the 2010 QHSR and, while acknowledging that producing the first QHSR was a "massive undertaking" recommended that the next QHSR leverage lessons learned from the 2010 QHSR to strengthen its planning and risk management efforts. A focus of GAO's recommendations was on fostering greater stakeholder engagement—by building more time for obtaining feedback and input and examining additional mechanisms to obtain stakeholders' feedback.[188] GAO also recommended integrating risk information into decision-making regarding the priorities set forth in the next comprehensive assessment.[189]

The second QHSR was completed in 2014. According to GAO, this assessment was an improvement over the 2010 submission, insofar as it reflects important steps that DHS took toward assessing homeland security risks and improving stakeholder involvement but that its failure to fully document the risk assessment or how its analyses were synthesized to generate results limited reproducibility and defensibility of the results.[190] With respect to stakeholder engagement with HSE partners, GAO concluded that the collaboration could be improved, particularly when it comes to fostering interactive communication and feedback.[191]

Findings & Recommendations:

Since enactment of the *9/11 Commission Act*, DHS has made steady progress at ensuring that the QHSRs that are produced reflect analysis regarding existing risks to the Nation and are informed by engagement with HSE partners. The degree to which such an assessment can provide strategic value to the Department and its Federal and non-Federal partners is directly related to the rigor in its risk assessment and the robustness of stakeholder engagement efforts.

The 2018 QHSR is currently underway, and expected in December of 2017.[192] However, moving forward, the QHSR should be enhanced to provide a strategic foundation for decision-making regarding homeland security policy, program, and structure, section 2401 should be amended to—

- require DHS to carry out more robust stakeholder engagement, particularly with HSE partners;
- clarify that DHS is required to carry out a risk assessment to identify "threats to the assumed or defined national security interests of the Nation that were examined for the purposes of that [QHSR]"[193]; and

[188] *Quadrennial Homeland Security Review: Enhanced Stakeholder Consultation and Use of Risk Information Could Strengthen Future Reviews* (GAO-11-873). Washington, DC: U.S. Government Accountability Office, 2011.
[189] Ibid.
[190] Ibid.
[191] Ibid.
[192] "The 2018 Quadrennial Homeland Security Review," U.S. Department of Homeland Security, last modified November 17, 2016, accessed August 23, 2017, https://www.dhs.gov/2018-quadrennial-homeland-security-review.
[193] 9/11 Commission Act, 121 Stat. 545 (2007).

- require DHS to retain all documentation regarding stakeholder engagement and the risk model utilized to generate the risk assessment.

Recommendation: To facilitate these improvements to the law, H.R. 1297, the *Quadrennial Homeland Security Review Technical Corrections Act of 2017*, as introduced by Congresswoman Bonnie Watson Coleman (D-NJ) should be enacted into law.

H.R. 1297 includes provisions to require greater specificity on outreach to stakeholders, a risk assessment, and retention of documentation, including all written communications through technology, online communication, in-person discussions and the interagency process, and all information on how the communications and feedback informed the development of the review.[194] H.R. 1297 was approved by the House on March 21, 2017 by a vote of 415 to 0 and is currently pending in the Senate.

X. BIOSURVEILLANCE *(Sec. 1101)*

Background

Section 1101 of the *9/11 Commission Act* mandated the establishment of the National Biosurveillance and Integration Center (NBIC) by September 30, 2008 to enhance Federal capabilities to (1) "rapidly identify, characterize, localize, and track a biological event of national concern[195]"; (2) "disseminate alerts" across the Federal government and to State, local and tribal partners; and (3) "oversee the development and operation of the National Biosurveillance Integration System" (NBIS) (the network of Federal agencies that maintain surveillance systems and may have information helpful for decision-making during an event).[196] Further, the law requires Federal partners to "provide timely information to assist the NBIC in maintaining biological situational awareness" through the NBIS to the NBIC to assist in detection of a biological event of national concern "as early as possible."[197]

Even before the NBIC was stood up, it became apparent that full-achievement of the Center's complex and ambitious mission would be an extremely challenging undertaking. In July 2008, GAO testified that: "DHS has made progress making NBIC fully operational by September 30, 2008; however, it is unclear what operations the center will be capable of

[194] H. Comm. on Homeland Security, Quadrennial Homeland Security Review Technical Corrections Act of 2017, Report No. 115-41 (March 16, 2017).
[195] "Biological event of national concern" is defined as "an act of terrorism involving a biological agent or toxin; or a naturally occurring outbreak of an infectious disease may result in a national epidemic." 9/11 Commission Act, 121 Stat. 378 (2007).
[196] 9/11 Commission Act, 121 Stat. 375 (2007).
[197] 9/11 Commission Act, 121 Stat. 376-7 (2007).

carrying out at that point."[198] GAO observed challenges related to "defining what capabilities the center will provide once fully operational, formalizing agreements to obtain interagency coordination, and completing work related to the new information technology (IT) system."[199]

The following year, GAO found that the NBIC had made efforts to acquire data and establish governance bodies to support data collection, analysis, and communications but that it is not fully equipped to carry out its mission because its partner agencies have not provided the necessary data and personnel to effectively "leverage analytical expertise."[200] GAO explained that "[i]ntegrating biosurveillance data is an inherently interagency enterprise, as reflected by both law and NBIC's strategy for meeting its mission. NBIC is to help coordinate and support a community of federal partners for early detection and enhanced situational awareness."[201]

In the 2009 report, GAO made two recommendations to improve the program. First, GAO recommended that NBIC finalize a strategy "defining NBIC's mission and purpose, along with the value of NBIS membership for each agency," "addressing challenges to sharing data and personnel, including clearly and properly defining roles and responsibilities in accordance with the unique skills and assets of each agency," and "developing and achieving buy-in for joint strategies, procedures, and policies for working across agency boundaries."[202] Second, GAO recommended NBIC "establish and use performance measures to monitor and evaluate the effectiveness of collaboration with current and potential NBIS partners."[203] Then, in 2010, to underscore GAO's view that building and maintaining a national biosurveillance capability is an "inherently interagency enterprise," GAO recommended that the National Security Staff, in coordination with relevant Federal agencies, "(1) [e]stablish the appropriate leadership mechanism . . . to provide a focal point with authority and accountability for developing a national biosurveillance capability;" and "(2) [c]harge this focal point with responsibility for developing. . . a national biosurveillance strategy. . . ."[204]

In July 2012, the Obama Administration issued the National Strategy for Biosurveillance that made no direct mention of the NBIC but whose stated goal was to advance an "all-of-Nation approach" to unify national effort around a common purpose and establish new ways of thinking about providing information to enable better decision making.[205] In November

---

[198] *BIOSURVEILLANCE: Preliminary Observations of the Department of Homeland Security's Biosurveillance Program*, (GAO-08-960T) (Washington, DC: U.S. Government Accountability Office, 2008), 5, http://www.gao.gov/assets/130/120703.pdf .
[199] *Id* at 2.
[200] *BIOSURVEILLANCE: Developing a Collaboration Strategy Is Essential to Fostering Interagency Data and Resource Sharing*, (GAO-10-171) (Washington, DC: U.S. Government Accountability Office, 2009), 10, http://www.gao.gov/assets/300/299667.pdf.
[201] *Id.* at Highlights.
[202] *Id.* at 28-29.
[203] *Id.* at 29.
[204] *BIOSURVEILLANCE: Efforts to Develop a National Biosurveillance Capability Need a National Strategy and Designated Leader*, (GAO-10-645) (Washington, DC: U.S. Government Accountability Office, 2010), 46, http://www.gao.gov/assets/310/306362.pdf.
[205] The White House, *National Strategy for Biosurveillance*, (Washington, DC: July 2012), https://obamawhitehouse.archives.gov/sites/default/files/National_Strategy_for_Biosurveillance_July_2012.pdf

2012, the Department issued the NATIONAL BIOSURVEILLANCE INTEGRATION CENTER STRATEGIC PLAN (2012 NBIC STRATEGIC PLAN) that included an extensive "path toward implementation" section setting forth Federal actions for the period FY14 through FY18.[206]

In September 2015, GAO issued a report that compared the realities of NBIC operations against what was envisioned in both the *9/11 Commission Act* and the 2012 NBIC STRATEGIC PLAN.[207] The report analyzed the actions and challenges associated with the three roles envisioned for the NBIC. With respect to its analyzer role, "GAO found that NBIC produces reports on biological events using open-source data, but faces challenges obtaining data and creating meaningful new information" and that NBIS partners cited "legal and regulatory restrictions" as barriers to sharing information with DHS.[208]

With regard to NBIC's coordinator role, GAO acknowledged that the NBIC had procedures and activities to coordinate with partners, such as daily and biweekly calls, but "faces challenges related to the limited partner participation in the center's activities, lack of partner personnel detailed to NBIC, and competing structures for convening Federal partners."[209] Finally, with respect to its innovator role, the NBIC had undertaken some pilot projects to examine "the use of social media data to identify health trends, but faces challenges prioritizing developmental efforts."[210] GAO concluded that the NBIC "faces challenges that limit its ability to enhance the national biosurveillance capability" and it is unclear how NBIC adds value.[211] Ultimately, GAO provided a series of options for NBIC and Congress to consider to better clarify NBIC's mission in a manner that might improve its value to the interagency.[212]

In October 2015, the Blue Ribbon Study Panel on Biodefense issued a bipartisan report entitled "A National Blueprint for Biodefense: Leadership and Major Reform Needed to Optimize Efforts" that, among other things, called authority to be vested in the Office of the Vice President of the United States to "control, prioritize, coordinate, and hold agencies accountable for working toward common national biodefense."[213] With respect to the NBIC, the Panel concluded that "[d]espite the best of intentions, DHS has been unable to meet this mandate, in large part because other federal agencies were not required in the statute to share data or information with DHS," and that "[t]he lack of required interagency sharing of surveillance data means that NBIS can only function properly if the White House forces it to work."[214]

---

[206] U.S. Department of Homeland Security, *National Biosurveillance Integration Center Strategic Plan*, (Washington, DC: November 2012), https://www.dhs.gov/sites/default/files/publications/nbic-strategic-plan-public-2012.pdf.
[207] *BIOSURVEILLANCE: Challenges and Options for the National Biosurveillance Integration Center*, (GAO-15-793). (Washington, DC: U.S. Government Accountability Office, 2015), http://www.gao.gov/assets/680/672732.pdf .
[208] *Id.* at Highlights.
[209] Ibid.
[210] Ibid.
[211] Ibid.
[212] *Id.* at 36-44.
[213] Blue Ribbon Study Panel on BioDefense, *A National Blueprint for Biodefense: Leadership and Major Reform Needed to Optimize Efforts*, (October 2015), vii, https://s3.amazonaws.com/media.hudson.org/20151028ANATIONALBLUEPRINTFORBIODEFENSE.pdf.
[214] *Id.* at 31.

Findings and Recommendations

Though DHS stood up the NBIC as required under the *9/11 Commission Act*, it has not been able to fulfill its core missions. NBIC's challenges have resulted from two separate, yet interrelated problems: within DHS, its Office of Health Affairs (OHA), which is charged with overseeing the NBIC, lacks the statutory authority to compel other Federal agencies to share information and expertise, and OHA has been unable to develop a framework for voluntary compliance that would incentivize information sharing and define the roles and responsibilities of Federal partners. Following the 2015 GAO Blue Ribbon Study Panel reports, OHA did not appear to contemplate or seek from Congress significant operational, mission, or budgetary changes that could have revamped the program. Ultimately, it is unclear whether NBIC implemented any changes in response to either reports' findings and appears to have continued to operate in a steady state for the past two years.

The Administration's FY18 budget proposes eliminating the NBIC, which has been funded at around $10 million a year since its inception. In the past, the Committee has expressed reservations about funding NBIC, given its questionable value to the Federal interagency, as chronicled by GAO and the Blue Ribbon Study Panel. That said, State and local governments as well as the National Security Council have expressed – albeit anecdotally – that NBIC's biosurveillance products have value.

Accordingly, it would be wrong to eliminate the program without undertaking robust discussions with all stakeholders about not only the potential impacts of the elimination of the NBIC on Federal, State, and local partners but also a path forward for biosurveillance at DHS.

Recommendation: Congress should direct a review of NBIC to fully ascertain its value to Federal, State, and local stakeholders. Additionally, Congress should consider whether other entities, such as the Department of Energy's National Laboratories, might be better equipped to carry out aspects of the complex biosurveillance mission set forth for the NBIC under the *9/11 Commission Act*.

The struggles experienced by NBIC – the inability of the Federal government to coordinate effectively in the biodefense space – is a symptom of a larger problem: lack of leadership. Without an individual empowered by the White House to encourage the exchange of the kind of raw data necessary to inform meaningful biosurveillance products, OHA has not been able to ensure that NBIC is able to access the data it needs to carry out its mission.

During the George W. Bush Administration, the Special Assistant to the President for Biodefense served as the chief advisor to the President on biodefense issues and coordinated

Federal biodefense and biosurveillance activities. No such position exists today, and many biodefense experts, including the Blue Ribbon Study Panel, have identified this leadership vacuum as a major barrier to biodefense and gains in biosurveillance. Those concerns came to a head in fall 2014 when the Federal government struggled to carry out a well-coordinated response to U.S. Ebola cases, with President Barack Obama ultimately appointing an Ebola Czar to improve the efficacy of Federal efforts. Although the Ebola situation was not the result of terrorism, it did raise important questions about leadership and coordination of policies related to biological events – be they naturally-occurring or man-made.

Recommendation: The Administration should designate a high-ranking individual in the White House to coordinate biosurveillance and biodefense activities across the Federal government.

As noted above, the Blue Ribbon Study Panel on Biodefense recommended in 2015 that biodefense activities be institutionalized in the Office of the Vice President, a Biodefense Coordination Council be established at the White House, and that biodefense budgeting be unified under the Vice President's authority.[215] Putting aside the question of whether a Vice President is the best Federal official to coordinate Federal biodefense efforts, it is critical that there be an individual at the White House—with the authority to lead—who is responsible for coordinating Federal efforts.

[215] *Id.*

ACRONYMS AND ABBREVIATIONS

ACAS	Air Cargo Advance Screening
ADIS	Arrival and Departure Information System
AME	Emanuel African Methodist Episcopal Church
ANPRM	Advance Notice of Proposed Rulemaking
APTA	American Public Transportation Association
AQAP	Al Qaeda in the Arabian Peninsula
BASE	Baseline Assessment for Security Enhancement
CBP	Customs and Border Patrol
CCSP	Certified Cargo Screening Program
COMTs	Communications Unit Technicians
CSI	Container Security Initiative
DNDO	Domestic Nuclear Detection Office
ESTA	Electronic System for Travel Authorization
FBI	Federal Bureau of Investigations
FEMA	Federal Emergency Management Agency
FirstNet	First Responder Network Authority
GAO	Government Accountability Office
HSAS	Homeland Security Advisory System
HSDN	Homeland Security Data Network
HSE	Homeland Security Enterprise
HSGP	Homeland Security Grant Program
HSIN	Homeland Security Information Network
I&A	Intelligence and Analysis
IDENT	Automated Biometric Identification System
IECGP	Interoperable Emergency Communications Grant Program
JTTF	Joint Terrorism Task Force
MTI	Mineta Transportation Institute
NBIC	National Biosurveillance Integration Center
NBIS	National Biosurveillance Integration System
NECP	National Emergency Communications Plan
NII	non-intrusive inspection
NSGP	Nonprofit Security Grant Program
NTAS	National Terrorist Advisory System
NTC	National Targeting Center
OHA	Office of Health Affairs
OIG	Office of Inspector General
OPSG	Operation Stonegarden

POE	Port of Entry
PRD	Personal Radiation Detectors
QHSR	Quadrennial Homeland Security Review
RIID	Radiation Isotope Identification Devices
RPM	Radiation Portal Monitors
RFI	Request for Information
SCIP	Statewide Communications Interoperability Plan
SFI	Secure Freight Initiative
SHSGP	State Homeland Security Grant Program
SLTT	State, local, tribal and territorial
SWICs	Statewide Interoperability Coordinators
TSA	Transportation Security Administration
TSGP	Transit Security Grant Program
UASI	Urban Area Security Initiative
VIPR	Visible Intermodal Protection and Response
VWP	Visa Waiver Program

Staff report authored by the Democratic Staff of the Committee on Homeland Security
U.S. House of Representatives
Washington DC 20515
202-226-2616
Democrats-homeland.house.gov