December 2017

FINAL REPORT FROM THE REPUBLICAN MEMBERS OF THE

TASK FORCE ON DENYING TERRORISTS ENTRY TO THE UNITED STATES

HOMELAND SECURITY
COMMITTEE

HOMELAND SECURITY COMMITTEE
REPUBLICAN MEMBERS OF THE TASK FORCE

on

DENYING TERRORISTS ENTRY INTO THE UNITED STATES

Chairman Michael McCaul
Texas

Republican Members

Rep. Michael Gallagher, Task Force Chairman
Wisconsin

Rep. Clay Higgins
Louisiana

Rep. John H. Rutherford
Florida

Rep. Thomas A. Garrett, Jr.
Virginia

Rep. Brian Fitzpatrick
Pennslyvania

Rep. John M. Katko, Ex Officio Advisor
New York

CONTENT

Introduction

Overview

Appendices

EXECUTIVE SUMMARY

Task Force on Denying Terrorist Entry into the United States

Given the terrorism threat currently facing the United States, the House Homeland Security Committee established the Task Force on Denying Terrorists Entry into the United States (the Task Force) in February 2017. Chairman McCaul (R-TX) and Ranking Member Thompson (D-MS) appointed Rep. Mike Gallagher (R-WI) and Rep. Bonnie Watson Coleman (D-NJ) to lead a bipartisan group of lawmakers. In addition to following up on the work done by the Committee's previous bipartisan Task Force, this new Task Force was charged with: examining how terrorists might infiltrate the homeland; identifying challenges with current U.S. government information sharing and vetting procedures; reviewing the screening agencies' structure and bureaucracy; and providing substantive recommendations to fix any weaknesses in these systems.[1]

However, days before finalizing this report, our Democratic colleagues informed us that they did not agree to several recommendations that were previous areas of consensus, and would no longer agree to make this report bipartisan.

The Current Threat

The conflict in Iraq and Syria represents the largest mobilization of foreign fighters in history, surpassing the Afghanistan-Soviet conflict in the 1980s, which was believed to have mobilized between 5,000 to 20,000 foreign fighters.[2] More than 40,000 fighters, including approximately 5,000 Europeans, have traveled to Iraq and Syria to join groups such as the Islamic State of Iraq and Syria (ISIS).[3] It has been widely reported that many of these foreign fighters have traveled back to the West from Iraq and Syria further radicalized and equipped with the knowledge and battlefield experience necessary to perpetrate successful terrorist attacks. As former Secretary of Homeland Security John Kelly warned, returning foreign fighters "have learned how to make IEDs, employ drones to drop ordnance, and acquired experience on the battlefield that by all reports they are bringing back home."[4]

Exacerbating the overall threat is the reality that terrorists no longer need to travel to the conflict zone to receive orders and then execute attacks. ISIS has turned to cyber space to further its existence, attempting to create a "virtual caliphate" in place of a physical one. The group violates the United States' and the West's digital borders on a daily basis, exploiting the Internet to inspire, radicalize, and recruit followers. The group has also been able to exploit technology, such as encrypted apps, to provide guidance and instructions to followers for carrying out attacks thousands of miles away. Even as it continues to lose territory in Iraq and Syria, ISIS will continue to work through its propaganda and communication channels to recruit lone wolves who will act on senior ISIS leader Abu Mohammad al-Adnani's message to kill Western disbelievers "in any manner or way, however it may be" with any weapon available.[5]

The large number of European foreign fighters, coupled with Europe's counterterrorism challenges, present a direct threat to the U.S. homeland. Many European security services and law enforcement agencies are overwhelmed by the magnitude and dynamism of the threat and they have struggled to identify, track, and share information related to their citizens that have been radicalized and/or traveled to Iraq and Syria. The fact that the majority of European fighters come from Belgium, France, Germany, and the United Kingdom—all Visa Waiver Program (VWP) countries—further underscores the seriousness of this threat.[6]

Results of the Review

The Task Force identified seven challenges in America's screening and vetting framework prior to an individual's arrival in the homeland:

Information Sharing

Challenge: Thousands of foreign fighters have transited between the conflict zone and the West, and it will require an immense information sharing effort between the military, national security agencies, law enforcement services, and foreign partners to locate and track as many of them as possible. However, there are existing interoperability, legal, technical, and capacity challenges that hinder current information sharing efforts.

Recommendation: To overcome existing information sharing hurdles, Congress and the Executive Branch must cooperate to provide additional funding, personnel, and technology in support of both interagency and foreign partner information sharing. In the interim, the Executive Branch should continue its use of interagency embeds and task forces to enhance the U.S. government's information sharing efforts.[7] The U.S. government should also continue to increase engagement with foreign partners to establish permanent information sharing relationships and agreements.

Challenge: The process by which an individual seeking to come to the United States obtains authorization to travel and is ultimately admitted to this country involves numerous federal law enforcement and intelligence agencies. Each of these agencies has its own authorities and maintains holdings essential to the vetting and screening process. Over the years since 9/11, it would be expected that some unnecessary duplication, agency stove-piping, and gaps in the screening and vetting infrastructure have developed.

Recommendation: The Executive Branch should conduct a review of the current screening and vetting bureaucracy to ensure each entity involved in the process is in its proper "lane of the road" and fully executing its statutory responsibilities and internal policies and procedures. Such a review should help promote the best possible information sharing, security, coordination, and efficiency. The Executive Branch should also work with Congress to address any issues that require legislation.

Screening and Vetting

Challenge: The Visa Security Program (VSP) has allowed the Department of Homeland Security (DHS) to push its screening operations out to consular posts abroad by having U.S. Immigration and Customs Enforcement (ICE) agents vet individuals before they are granted a visa. U.S. Customs and Border Protection's (CBP) National Targeting Center (NTC) also plays a significant role in supporting state side vetting of visa applications. Limited resources, however, have hindered the VSP's development and expansion to additional high-risk, overseas posts.

Recommendation: DHS should continue to expand VSP to additional high-risk consular posts and should work with Congress to prioritize additional funding for the program. Congress should also examine other avenues to help fund the program's expansion. In cases where VSP expansion faces challenges, DHS should remotely perform the functions of the program via a reach-back capability.

Challenge: As technology has continued to develop and more of our lives move online, a wealth of valuable information has become available, primarily on social media, that can be used to screen and vet foreign nationals seeking to come to the United States. In addition, information gathered from social media can be just as valuable as the biographic information traditionally used for screening and vetting. The U.S. government is not fully utilizing social media information for screening and vetting purposes.

Recommendation: DHS and the Department of State should expand the use of social media information for screening and vetting foreign nationals.[8] The federal government should also work with the private sector to develop technology to better incorporate social media into the screening and vetting process. Congress and the Executive Branch must work together to address resourcing needed for personnel, management, research, and acquisition of social media tools to improve the utility of social media information sources. (This recommendation reflects Committee passed legislation, H.R. 2626, the Strong Visa Integrity Secures America Act, which passed the Committee by voice vote on July 26th, 2017.)

Challenge: The Terrorist Screening Center (TSC) is a multi-agency body that administers the Terrorist Screening Database (TSDB).[9] Despite having a mission that is more in line with that of DHS, the TSC currently falls under the auspices of the Federal Bureau of Investigation (FBI). Furthermore, despite the key role it plays in facilitating information sharing, the TSC is not authorized in statute.

Recommendation: The Government Accountability Office should assess the existing relationship between the TSC and the NTC to determine whether the functions of the TSC should be transferred to DHS, especially since the TSC's role as an information sharing facilitator directly aligns with the DHS core missions of screening and vetting and DHS is the largest consumer of TSDB data.[10] Such a review should also focus on changes to either entity that could be made to enhance security, efficiency, and coordination between the centers. Any changes that produce efficiencies would be in line with Executive Order 13781, the Administration's executive order on efficiency.[11]

Challenge: Given the challenge posed by the increased sophistication of our enemies, it is critical our system is agile enough to stay ahead of emerging threats. Although a baseline exists, the level of screening and vetting a foreign national receives is currently based on periodic threat assessments that determine the relative risk for each type of applicant (immigrant, non-immigrant, refugee, etc.). Furthermore, continuous screening of foreign nationals already in the United States is not standard practice, presenting a vulnerability related to a foreign national that becomes a threat after already entering the United States.

Recommendation: DHS should conduct internal assessments on the current screening and vetting procedures for each type of applicant to ensure all foreign nationals are receiving the proper level of scrutiny prior to being admitted into the United States. DHS should also build upon and expand, in a risk based manner, continuous screening initiatives to ensure individuals who may pose a threat receive the proper and lawfully permitted scrutiny throughout their entire travel or immigration lifecycle. (This recommendation reflects Committee passed legislation, H.R. 2626, the Strong Visa Integrity Secures America Act, which passed the Committee by voice vote on July 26th, 2017.)

Visa Waiver Program

Challenge: In order to participate in the VWP, countries must enter into terrorism and criminal information sharing agreements with the United States. However, some VWP countries do not have the technical capability or legal authorities needed to engage in automated and continuous information sharing. Some VWP partners also do not share biometric information and traveler data, such as Passenger Name Record (PNR) data or Advance Passenger Information (API), with the United States, or inconsistently share information with international entities such as Europol and INTERPOL. Furthermore, in some VWP countries, the information being exchanged is not consistently used by their domestic security services for screening and vetting, while other partners are unable to use all available data, including PNR and API, to enhance their own capabilities.

Recommendation: DHS should leverage the legal requirements of VWP, especially those in the *Visa Waiver Program Improvement and Terrorist Travel Prevention Act of 2015* (Public Law 114-113), to ensure our VWP partners continue their efforts to share biometric and biographic information on known and suspected terrorists (KST) when available, increase their overall information sharing with international

entities, more robustly exchange and utilize PNR and API data relevant to U.S. security, and utilize the information being exchanged as part of their screening and vetting processes. The U.S. government should also offer to continue to work with our VWP partners who request further assistance to help them develop the capabilities needed to utilize API and PNR to bolster their screening and vetting capabilities.

NOTES ON METHODOLOGY

The Task Force conducted the investigation over a six-month period. Its final report is based on briefings, meetings, domestic and foreign site visits, and analysis of official government documents. A summary of the Task Force's activity can be found in Appendix I. The Task Force spoke with current and former federal officials throughout the national security community and all relevant departments and agencies. The group also consulted with outside experts and foreign officials.

The Task Force examined U.S. government efforts with the most relevance to denying terrorist entry in to the homeland (e.g. the Visa Waiver Program, traditional visa screening, and refugee and asylee screening). The review specifically focused on government efforts to screen and vet individuals prior to entering the country. Where practicable, the Task Force has tried to cite publicly available sources, due to the fact that many of the Task Force's briefings were classified or sensitive in nature. However, some material is cited anonymously in cases where individuals were assured confidentiality in order to discuss issues more freely. Prior to publication, the final report was shared with the main departments and agencies that contributed to and assisted in the review. The Task Force incorporated their feedback where appropriate.

PREVIOUS COMMITTEE TASK FORCE

In response to the unprecedented number of foreign fighters, including thousands of Westerners flocking to Iraq and Syria to join groups such as ISIS, the Committee created a bipartisan *Task Force on Combating Terrorist and Foreign Fighter Travel* in February 2015. This Task Force was charged with assessing U.S. government efforts to obstruct terrorist travel to and from the conflict zone. The final Task Force report contained 32 key findings, along with accompanying recommendations. Some of those recommendations were incorporated into legislation and signed into law during the 114th Congress, greatly enhancing the U.S. government's ability to counter the threat posed by foreign fighters.

The flow of foreign fighters into the conflict zone has now essentially come to a complete halt.[12] However, as ISIS loses its last strongholds in Iraq and Syria, the terrorist diaspora will continue, and some foreign fighters could seek to return to their home countries, including in the West, to carry out attacks. As such, it is important that each individual seeking to enter to United States is thoroughly screened and vetted, making the current *Task Force on Denying Terrorists Entry into the United States* a natural extension of the Committee's previous Task Force.

THREAT LANDSCAPE

Since 2011, national security experts noted a significant uptick in the recruitment and radicalization of Europeans and Americans by terrorist organizations. This unprecedented growth in terrorist recruitment has been primarily driven by ISIS. Illustrating the group's ability to draw recruits, according to the 2016 State Department Country Reports on Terrorism, ISIS has drawn roughly 40,000 foreign fighters, from 120

countries, since 2011.[13] Thousands of those foreign fighters came from Europe and a few hundred came from the North America.[14]

The Terrorist Diaspora

Alarmed by the continued defeat of the Iraqi army by ISIS fighters and the group's declaration of a caliphate, President Obama agreed to requests from the Iraqi government for airstrikes against ISIS in northern Iraq in August of 2014.[15] A month later, the United States launched Operation Inherent Resolve, an alliance of Western and Gulf states with the goal of providing air support, along with special operations forces and expertise, to local Iraqi and Kurdish forces, who would undertake ground combat operations against ISIS insurgents in Iraq and Syria.[16] The operation led to slow but steady losses for the terrorist group.

By 2016, it became clear that ISIS' strongholds in Iraq and Syria would fall. In July of 2017, anti-ISIS forces had liberated Mosul, Iraq's second largest city and ISIS' most important in Iraq. In October of 2017, the U.S.-backed Syrian Democratic Forces (SDF) retook Raqqa, ISIS de facto capital.[17] Finally, in November of 2017, the Syrian army retook Deir Ezzor, the last major ISIS stronghold in Syria. These military victories have drastically shrunk the group's numbers and the territory they control. According to the official spokesman of Operation Inherent Resolve, nearly all of the territory ISIS controlled has been retaken and 7.5 million people have been liberated.[18] The rate of foreign fighters leaving the conflict has declined sharply since 2015, mostly because of the difficulty fighters face in leaving the conflict zone. Nonetheless, loyal fighters who stay in the region will likely hide, rearm and recuperate—going underground for a period before reemerging to fight the next phase of the insurgency. Still others may escape to ISIS' many provinces, enabling ISIS to regroup and continue its recruitment and fight against the West.[19] Others may choose to return home and potentially commit future attacks outside the caliphate or fade back into society.

Returning Foreign Fighters

In April 2017, then-DHS Secretary John Kelly stated that as ISIS continues to lose its safe haven in Iraq and Syria, "the expectation is that many of these 'holy warriors' will survive departing for their home countries to wreak murderous havoc in Europe, Asia, the Maghreb, the Caribbean, and the United States."[20] Secretary Kelly's message highlights the significant threat posed by returning ISIS fighters who seek to leave the Middle East theater. While some returned fighters remain quiet, U.S. officials are most concerned about ISIS operational members that seek to plant themselves in the West or create new networks and cells abroad.[21] These fighters are the most deadly, hardened, experienced, and committed to carrying out terror attacks in other parts of the world to spread ISIS philosophy. Furthermore, it is a challenge for law enforcement globally to keep pace with the large number of fighters returning home.[22]

Some experts assert returned foreign fighters are more likely to later pursue an attack, especially after having received training and battlefield experience.[23] According to National Counterterrorism Center (NCTC) Director Rasmussen, more than half of the terrorism related fatalities in Europe since 2015 were caused by attacks involving returning foreign fighters.[24] This violence is not spontaneous, it is committed in furtherance of ISIS' goals. While attacks have taken place worldwide, attacks in Europe have drawn particular scrutiny in terms of their implications for the security of Americans and of the U.S. Homeland. The attacks in Paris in November 2015, which killed 130 people, and the airport and subway bombings in Brussels in March 2016 that claimed 32 lives, are deadly examples of ISIS' planned infiltration of the West.[25] The Paris attacks at the Bataclan Concert Hall and in restaurants in Paris' 11th District involved seven individuals from France and Belgium who had travelled previously to Syria to fight for the Islamic State. Further investigation by French authorities revealed that a total of 30 individuals were involved in the attacks, 16 of whom had been foreign fighters in Iraq or Syria.[26] Some of the attackers were able to sneak back into Europe by hiding among the nearly one million refugees who have come to the continent

from Syria.[27] However, Director Rasmussen also testified that "we have not seen ISIS successfully replicate this attack method in more than a year, probably because of increased border security and information sharing among our European partners."[28]

Returned foreign fighters are also strategically positioned to recruit new supporters on behalf of ISIS. There is evidence that some have functioned as undercover operatives, using new converts with no known ties to Islamist groups as go-betweens, linking the operative with those willing to carry out attacks.[29] Operatives, as well as new recruits, remain connected via the web with ISIS remnants around the globe that provide directions and resources for attacks.[30] Acting Secretary of Homeland Security Elaine Duke underscored this reality in testimony before the Senate in 2017, stating that "changes in technology have made it easier for [terrorists] to plot attacks in general, to radicalize new followers, and to recruit beyond borders."[31]

The success of ISIS' external operations in Europe, and their ability to recruit European locals, culminated in the May 2016 announcement by deceased ISIS spokesman al-Adnani that aspiring fighters in the West should focus on attacks at home.[32] Despite the group's continued losses on the battlefield, according to Central Intelligence Director (CIA) Director Mike Pompeo, ISIS has maintained its external operations capabilities, in part by moving its recruitment efforts and plot guidance into the digital realm.[33] This is evidenced by the fact that some attacks in recent years initially thought to be disconnected from the larger group, so called "lone wolf" attacks, turned out to be remotely guided plots linked to the Islamic State.[34]

Despite the recent rate of attacks in Europe, the United States remains a top target for terrorists. As Federal Bureau of Investigation (FBI) Director Christopher Wray explained to the Committee in November of 2017, the FBI "continues to identify individuals who seek to join the ranks of foreign fighters traveling in support of ISIS, as well as homegrown violent extremists who may aspire to attack the United States from within."[35] On May 13, 2017, Hamza bin Laden, the son of 9/11 mastermind Osama bin Laden, released a recording asking believers to prioritize American and Jewish targets by "diligently inflicting crippling losses on those who have disbelieved." In his video to followers, he promises imminent attacks and plays footage of the 1993 World Trade Center attack and Fort Hood, Texas attacker Maj. Nidal Malik Hasan.

Indeed, there have been 147 homegrown jihadist cases in 28 states and District of Columbia since 2014.[36] Of note, in August 2017, Parveg Ahmed, 22, a naturalized U.S. citizen from Queens, New York, was arrested for attempting to provide material support to ISIS. Ahmed allegedly travelled to Saudi Arabia in an attempt to continue on to ISIS-held territory in Syria.[37] The same month, the FBI arrested Uzbek citizen Dilshod Khusanov, living in Chicago, for conspiring with a network of six others to provide support to ISIS and the al-Nusrah Front.[38] Most recently, in October 2017, Sayfullo Habibullaevic Saipov, a legal U.S.-resident originally from Uzbekistan, who claimed to have been inspired by ISIS, drove a rented truck down a bicycle lane in New York City, killing eight and wounding thirteen.[39]

CURRENT SCREENING AND VETTING SYSTEM

In response to the September 11, 2001 terrorist attacks, and other events thereafter, the U.S. government has continually revamped the system of screening and vetting foreign travelers to enhance our ability to identify and interdict terrorists seeking to enter the United States. This included creating a centralized watchlisting enterprise to share terrorism information across the relevant U.S. authorities and with foreign partners; employing a multilayered approach to screen and vet travelers before, en route, and after they enter the United States; and extending screening and vetting capabilities beyond our borders through security partnerships such as the Visa Waiver Program, the Visa Security Program, and CBP

Preclearance operations.[40] However, in spite of these advances, challenges in our screening and vetting systems remain.

Watchlisting and Information Sharing

The 9/11 Commission identified poor information sharing as one of the critical vulnerabilities that allowed the 9/11 hijackers to enter the United States and carry out their attacks. Although various components of the U.S. intelligence and law enforcement community had significant amounts of information on their identities, prior travel history, and nefarious ties, this information was not available across the U.S. government, including to entities charged with the screening and vetting of travelers. [41]

One of the 9/11 Commission's key recommendations was the creation of an effective mechanism for sharing terrorism information across the U.S. government. This recommendation led to the creation of the NCTC, which is responsible for maintaining the Terrorist Identities Datamart Environment (TIDE), the "US government's central repository for information on international terrorist identities." TIDE includes all U.S. government information, as permitted by law, related to the identities of known or suspected terrorists. [42] The information in TIDE is then used to compile the terrorist watchlist, known officially as the TSDB. This watchlist is currently administered by the TSC, a multi-agency body administered by the FBI and staffed by temporary staff from the Department of Justice (DOJ), DHS, State, and other U.S. law enforcement and intelligence agencies.

Portions of the TSDB are exported to data systems in federal agencies that perform screening activities such as background checks, reviewing the records of passport and visa applicants, official encounters with travelers at U.S. border crossings, and air passenger screening. Portions of the TSDB are also shared with select foreign partners to assist with their border screening and law enforcement investigations, enhancing the U.S. government's ability to detect and interdict terrorists before they reach the homeland. [43]

While the existing watchlisting enterprise represents a vast improvement compared to our pre-9/11 capabilities, interoperability issues among U.S. agencies—and with our foreign partners—continue to hinder efforts to make valuable information available for frontline screening and vetting in a timely manner. Not only is this a bureaucratic challenge—given the number of separate government agencies and components involved—but legal, capacity, and technical issues exist as well.[44]

Visa Screening and Vetting

Our ability to effectively use intelligence and law enforcement information to detect and interdict terrorists before they enter the homeland depends on having a robust screening and vetting system for all foreign travelers at each step in the admission process. Every decision to issue a visa or a travel authorization, and to admit a foreign national into the United States, must be based on national security first and foremost.[45]

The visa process is administered by the State Department at embassies and consulates abroad. State Department consular officers use a multitude of tools to screen visa applications, and the vast majority of applicants are interviewed in person by a consular officer. During the interview, consular officers focus on verifying the applicant's identity, determining qualifications for the applicant's particular visa category, and inquiring into any possible ineligibilities, including links to terrorism, crime, or other security concerns. In addition to the in-person interview, the visa process also includes screening and vetting the applicant's information against key U.S. government intelligence and law enforcement databases, including TIDE and the TSDB. The State Department conducts further screening of biometrics collected at the interview and, if the initial vetting or interview reveal any concerns, additional in-depth vetting by U.S. law enforcement and intelligence agencies. No visa can be issued unless all relevant concerns are fully resolved.

At certain high threat posts, ICE, through the VSP deploys Visa Security Units (VSU) composed of Homeland Security Investigations (HSI) special agents. VSUs provide advice and training to State Department consular officers based on specific security threats, review visa applications, and conduct additional investigations into specific applicants, if warranted. These ICE agents overseas are supported by the U.S.-based Pre-Adjudicated Threat Recognition and Intelligence Operations Team (PATRIOT). PATRIOT is an interagency coordination effort to conduct advanced visa application vetting and enhance visa security. Participating agencies include DHS, CBP, ICE, and the State Department. PATRIOT provides the ability to screen pre-adjudicated visa applicants against DHS holdings, and uses ICE and CBP systems to return one overall DHS response to the State Department regarding any potential concerns associated with a visa applicant. Currently, there are 34 post locations receiving PATRIOT responses.[46]

Similarly, all foreign nationals wishing to settle in the United States permanently are required to have an approved immigrant benefit application and apply for an immigrant visa before they can travel to the United States. U.S. Citizenship and Immigration Services (USCIS) adjudicates all immigration benefit applications, which includes background and security checks against law enforcement, intelligence, and other federal databases and holdings. When information indicates a potential national security, fraud, or public safety concern, adjudicators refer the case to the Fraud Detection and National Security Directorate (FDNS) for further vetting. FDNS Immigration Officers will examine the details of the application and determine what additional vetting may be necessary to obtain a complete understanding of the concern. As part of the vetting process, FDNS officers also seek and share information with law enforcement agencies and other U.S. government partners as appropriate.

Finally, if new derogatory information comes to light after a temporary visitor or an immigrant visa is issued, the State Department uses its statutory authority to revoke visas and prevent dangerous travelers from reaching, or if they are already here, remaining in the U.S. homeland.

Visa Waiver Program

In light of the increased threat in Europe, the Visa Waiver Program (VWP) has emerged as a critical security tool in combating terrorist travel, while also facilitating legitimate travel.[47] Currently, nationals of the 38 VWP countries are allowed to travel to the United States for business or tourism for stays of up to 90 days (with certain exceptions) after applying and being approved through the CBP-administered Electronic System for Travel Authorization (ESTA). The traveler information provided through ESTA is vetted against key U.S. government intelligence and law enforcement databases, like the TSDB. It is important to note that simply having an approved ESTA does not guarantee entry to the United States. CBP officers make the final determination of admissibility (entry) to the United States at ports of entry and may cancel or deny a foreign national's ESTA at any time during travel. VWP travelers' fingerprints are also screened by CBP Officers as part of the final determination of admissibility (entry) to the United States. Approved ESTAs are subject to continuous vetting as long as they are valid and can be revoked based on the emergence of new derogatory information.

In return for participation in VWP, countries must prove that measurable and consistently high requirements are met, including: information sharing practices that enable the rapid relay of information concerning known and suspected terrorists and serious criminals; that lost and stolen passport information is consistently and reported in a timely manner; that robust border and travel document security practices are in place; and that effective traveler and migrant screening practices are standard operations. VWP countries also undergo regular, in-depth security assessments conducted by DHS in consultation with the Department of State to ensure compliance with these requirements. The bi-annual assessments evaluate the country's counterterrorism and law enforcement capabilities, immigration enforcement policies and procedures, passport production and issuance processes, border security, and traveler screening capabilities.

As needed, the review may also include a site visit where an integrated U.S. government team conducts thorough inspections of airports, seaports, land borders, and passport production and issuance facilities in the VWP country. The team also meets with the host government's counterterrorism, intelligence, law enforcement, border security, and immigration officials. Upon completion of the assessment, DHS is required to submit a report to Congress outlining the country's compliance with the VWP requirements.[48]

Under the *Visa Waiver Program Improvement and Terrorist Travel Prevention Act of 2015* (P.L. 114-113), VWP countries are now required to issue high-security electronic passports (e-passports); implement information sharing arrangements to exchange criminal and terrorist identity information; establish mechanisms to validate e-passports at each key port of entry; report all lost and stolen passports to INTERPOL or directly to the United States no later than 24 hours after the country becomes aware of the loss or theft; conclude a U.S. Federal Air Marshals agreement; collect and analyze Passenger Name Record (PNR) and Advance Passenger Data (API) to identify high-risk travelers; screen international travelers against the INTERPOL Stolen and Lost Travel Documents database and notices; report foreign fighters to multilateral security organizations, such as INTERPOL or Europol; and cooperate with the United States in the screening of refugees and asylum seekers.

Border Screening and Vetting

CBP plays a vital role in the identification of individuals who pose a national security concern to our homeland. CBP relies on advance traveler information, its pre-departure targeting operations, and its overseas footprint to address travelers of concerns long before they reach the physical borders of the United States. U.S. law requires all private and commercial air and sea carriers operating routes to, from, or through the United States to provide API data, and PNR when available, to CBP.[49] CBP uses API and PNR data to vet travelers against U.S. and international law enforcement and counterterrorism databases to identify high-risk individuals. Based on this vetting, CBP can issue "no-board" recommendations for individuals who will likely be deemed inadmissible upon arrival at a U.S. port of entry, before they get on a plane or vessel destined for the United States, and recommend that the State Department revoke the individual's visa. CBP also uses API and PNR data to identify individuals who may warrant additional scrutiny or screening prior to entering the United States.

When arriving at one of the 328 U.S. ports of entry, every individual is inspected by CBP. CBP Officers review entry documents, query CBP and other law enforcement databases, collect biometrics (including those of VWP travelers), and interview all travelers to determine the purpose and intent of their travel. If the traveler raises concern or suspicion, a CBP Officer can refer the individual for additional inspection prior to admission into the country.

After foreign travelers are admitted into the United States, CBP tracks their visas for the remaining validity using the Arrival and Departure Information System (ADIS). ICE further vets automated leads provided by ADIS, and takes enforcement actions on those determined to be priority overstay violators. While DHS has deployed a biometric entry system at airports, it has not yet implemented a biometric system to record the departure of individuals from the United States, as recommend by the 9/11 Commission and required under 8 U.S.C. 1365b.[50] Instead, DHS largely relies on biographic passenger manifest data transmitted by air carriers to identify potential overstays. DHS expects to have the capability to accept biometric departure data at the 20 busiest airports by the end of FY 2018. This biometric exit solution, in addition to existing checks of any biographic watchlist information, will assist CBP in identifying imposters and tying the information to existing records, strengthening current capabilities. Full biometric exit capability will improve the ability of DHS to more accurately and completely identify overstays.[51]

THE STATE OF EUROPEAN COUNTERTERRORISM

Counterterrorism gaps in some European countries continue to pose a threat to Europe's ability to protect itself and present a possible threat to the homeland because it is typically easier for a European citizen to travel to the United States. DHS and State Department personnel expressed concern to the Task Force that a European terrorist may slip through the cracks with less scrutiny.[52] According to NCTC Director Nicholas Rasmussen, of all the ISIS-linked attacks in Europe since 2015, "most attackers have been radicalized males with EU citizenship."[53] For example, some of the recent European terror attacks were perpetrated by individuals not on the radar of European counterterrorism officials. Given the lack of derogatory information on these individuals, and the fact they were European citizens, they may have been able to travel to the United States under the VWP.[54] However, while Europe has made significant progress in combatting terrorism, in addition to legal challenges, gaps remain in intelligence sharing both within and between European states, traveler screening, and border security.

Information Sharing within European States

As the terror threat continues to increase in both scope and complexity, information sharing within and among European states remains a key challenge for our European partners. In some key ways, Europe reflects the U.S. information sharing environment before 9/11, a situation characterized by institutional barriers to intelligence exchanges and interagency stove piping. In meeting with foreign partners, the Task Force heard about issues related to the walls that exist between European countries' military, law enforcement, and intelligence services, which limit the flow of information. Generally speaking, European militaries cannot provide information to European law enforcement entities, and European intelligence agencies can only pass information to law enforcement once certain conditions have been met. Often these conditions can be complex or hard to meet. Given these challenges, information within European states is often shared in an ad hoc and indirect manner.[55]

There are numerous examples that highlight how the failure of European militaries, law enforcement, and intelligence services to exchange information quickly and comprehensively poses a gap when it comes to interdicting suspected terrorists before they can commit acts of violence. In the fall of 2016, a sixteen-year-old German citizen of Moroccan descent, Safia S, was arrested after stabbing a police officer in the neck in the Hanover train station. Safia had been on the radar of intelligence authorities and had recently returned from Turkey where it was believed she tried to join ISIS.[56] Local authorities in Lower Saxony had been cataloging online propaganda videos of Safia and a radical German Islamist, and the state domestic intelligence office was even investigating the young girl for plotting an attack in November 2014. Despite a brief round of questioning, however, the German police let her go, having failed to analyze and contextualize the growing evidence that she had become dangerously radicalized.[57]

The case of Anis Amri, the Tunisian perpetrator of the December 2016 Berlin Christmas market attack, is another example of the threat posed by limited information sharing. In February of 2016, Amri came to the attention of German authorities based on his ties to a radical imam. His asylum application to remain in Germany was denied in June 2016, and a month later, he was arrested and transferred to a local detention center while his deportation was being processed. However, two days later, despite being under investigation by German security services, Amri was released.[58]

The United States has recognized the threat posed by barriers to information and has taken steps to assist our European allies with addressing this issue. INTERPOL Washington's National Central Bureau, the designated U.S. representative to INTERPOL, recently launched Operation Crosstalk, which is designed to break down the silos that currently exist between European military and law enforcement entities. As part of Operation Crosstalk, European militaries can send to their law enforcement counterparts at home, via

INTERPOL Purple Notices, information garnered from improvised explosive devices in theater, which may assist with or be relevant to active terrorism investigations.[59] Fingerprints pulled off of these devices can also be shared via INTERPOL Blue Notices.[60] INTERPOL and the U.S. National Central Bureau should continue to support these information sharing efforts and strongly encourage our European allies to continue working to break down walls that prevent important national security information from expeditiously flowing between the military, law enforcement, and intelligence.[61]

Information Sharing Between European States

There are several challenges to cooperation that have impeded the move towards integrated information sharing across Europe. These problems are the result of ineffective sharing structures, a reluctance towards interstate security cooperation, and divergent national resources and interests. Despite economic and political integration, national sovereignty remains a powerful force in European relations. States are sometimes reluctant to share information because they do not believe it to be in their national interest or are afraid sharing may compromise their sources.[62] States will sometimes share with one European partner but not another.[63] Moreover, predominantly for reasons of history, many European states are inherently suspicious of powerful, centralized intelligence services. However, because of the ability of threats to move quickly across the continent due to the Schengen Agreement, and the freedom of movement principle upon which the EU was founded, a willingness to share information with partners across the continent is vital to identifying and catching suspicious actors.[64]

European leaders are aware of the intelligence sharing problem and are taking steps to fix it. Europol recently launched the European Counterterrorism Center (ECTC) to act as a "unique European information hub" and facilitate information sharing among EU states.[65] According to Europol, more than 5,000 people from the EU have traveled to Iraq and Syria.[66] In a recent trip to Europol, the Task Force learned that these 5,000 individuals come from a larger pool of 45,000 individuals in ECTC databases who either attempted to travel to the conflict zone, are suspected of being foreign fighters, or are close associates of known foreign fighters.[67]

It should be noted, however, that ECTC was explicitly designed to separate law enforcement from intelligence, the opposite of the U.S. National Counterterrorism Center, and ECTC also has no intelligence collection powers or arrest authority, unlike organizations like the FBI. Rather, ECTC is a counterterrorism information hub, focused on connecting information that Europol Member States own and have chosen to share. ECTC also provides operational coordination and support, along with analytical support for counterterrorism investigations.[68] While the establishment of ECTC is undoubtedly a step in the right direction, its structure reinforces some of the already existing intra-European information sharing barriers. Since the information is owned by Member States, they can decide what to share and often will only share information they are comfortable with all Europol members having access to. Furthermore, if a country decides to remove information from ECTC, there is no recourse for Europol to regain access to that information. While ECTC is a good first step, Europe must do more to connect intelligence with law enforcement efforts, closing the gap that has led to missed terror suspects.

Security Service Resourcing Issues

In recent years, due to slow economic growth and divergent political priorities, some European countries have underfunded their law enforcement and intelligence services.[69] The unfortunate side effect of this underfunding is that some European security services have struggled to keep pace with the threat emanating from Iraq and Syria, and gathering the needed intelligence to disrupt terrorist cells and plots is becoming a more difficult task. While European authorities are confident that current foreign fighter flows into the conflict zone are near zero, the threat of those who have already returned is very concerning.[70] According to Europol's 2017 Terrorism Situation and Trend Report, foreign fighter returnees

"have increased proficiency in terms of carry out attacks, either under direction or independently." The report continued that "returnees will perpetuate the terrorist threat to the EU through radicalizing, fundraising and facilitation activities."[71]

As noted above, Europe's law enforcement community has challenges in keeping tabs on all suspects. For example, the U.K. has approximately 23,000 terror suspects on its intelligence radar.[72] In Germany, the Joint Counter-Terrorism Center (GTAZ), the country's main counter-terrorism intelligence hub, stated that they had evidence of over 550 individuals who made pro-ISIS statements in the state of North Rhine-Westphalia alone, and that it was impossible to closely monitor each individual.[73] Furthermore, Belgian police correctly identified some of the Brussels bombers prior to the attack, but had to drop its inquiry into them because it could not spare the resources for that particular case.[74]

In addition to working to mitigate the threat from returned foreign fighters, European security services are also grappling with the threat of "frustrated" fighters—radicalized individuals who can no longer travel to a warzone, but who nonetheless hope to carry out attacks in the name of ISIS.[75] Further compounding the threat, there is evidence that some returned foreign fighters are actively building a much larger network of radicalized individuals, many of whom are "frustrated" fighters, to carry out attacks against Westerners.[76] Those radicalized at home are even more likely to carry out an attack than a returned fighter, making them more dangerous in the short term.[77] Furthermore, newer recruits are increasingly younger, often avoiding scrutiny by law enforcement. Between September 2014 and December 2016, teens and preteens organized 34 plots against the West that were inspired or directed by ISIS.[78]

European officials also expressed concern to the Task Force regarding women and children returning from the conflict zone. Hans-Georg Maassen, the head of Germany's domestic intelligence agency, the Office for the Protection of the Constitution, explained this threat, stating that "there are children who have undergone brainwashing in the ISIS areas and are radicalized to a great extent…we also know that there are women one can rightfully call jihadists after living for years in [ISIS] areas where they identified strongly with [ISIS] ideology."[79]

European states have taken steps to try to address the resourcing issues related to their law enforcement and intelligence services. For example, while meeting with our European counterparts, the Task Force learned that one third of the Belgian military is currently performing constabulary duties. Meanwhile in France, 10,000 soldiers are walking police beats.[80] Following the Task Force's visit, additional public reporting underscored our findings.[81] While such measures may be an interim fix, these are not long-term solutions. Recent actions show that Europe understands the necessity of addressing these resource challenges. In the fall of 2016, Germany's budget commission approved the addition of thousands of new intelligence and law enforcement employees.[82] Belgium, in early 2016, also announced plans to nearly double its spending on police and intelligence.[83] The Task Force is encouraged by recent European investments in their security services, and urges our allies to continue providing these organizations the necessary resources to execute their missions.

Screening and Vetting Challenges

Since the outbreak of the Syrian conflict in 2011, Europe has experienced a significant flow of foreign fighters into the conflict zone. According to Europol's annual report on terrorism, more than 5,000 Europeans have traveled to fight with ISIS, and the Task Force learned that 1,700 have returned thus far.[84] Of the top 10 countries with the largest number of citizens and residents who have become foreign fighters, three are located in Europe (France, Germany, and the United Kingdom).[85] A high-ranking European official informed the Task Force that there are still approximately 2,600 European foreign fighters in Iraq and Syria.[86] Given the threat posed by those fighters still in the conflict zone, it is imperative that European countries be able to identify them if and/or when they attempt to return home. Without

thorough screening and vetting capabilities, Europe may be missing an opportunity to interdict these fighters before they return home where they may engage in violence or other terrorist activity.

The "Schengen Information System" (SIS) is the main system utilized to screen individuals entering the European Union. This system, however, falls short of a comprehensive, effective, and unified terrorist watch list like the United States' TSDB. Similar to some of the ECTC shortcomings, SIS is reliant on EU Member States placing information into the system. Both INTERPOL and the European Commission expressed concern to the Task Force that Member States may not be uploading all relevant information into SIS because they view security as a Member State issue or do not want to comprise ongoing investigations or other national interests.[87]

However, the European Union is taking a number of steps to bolster its vetting and screening efforts. According to the European Commission, there are plans to develop a exit system at all Schengen borders. This system will include fingerprints and photographs of all third country nationals. Development began in the fall of 2017, and the system should be completed by 2020. Work is also underway to create the European Travel and Information Authorization System (ETIAS)—a system that is comparable to the United States' ESTA. The European Commission expects there to be a political agreement on the development of ETIAS by the end of 2017, and development will begin in 2018 with an expected completion date of 2020 or 2021. Finally, the European Commission is in the process of putting forth a proposal for a "European search portal." Use of the portal will be mandatory for all EU states and ensure there are parallel searches of all EU-wide systems when screening and vetting individuals seeking to enter to the Schengen Area.[88]

While Europe is making strides toward improved screening and vetting in the coming years, operational gaps still exist. For example, according to U.S. officials overseas, only 10 percent of the records in SIS have fingerprints associated with them. Furthermore, the system lacks the ability to support automatic fingerprint recognition.[89] For years, European nationals were not screened against important databases like SIS when they returned to the EU because of a rule forbidding systematic screening of EU citizens. As of April 2017, however, the EU has mandated systematic checks of all individuals, including EU nationals, against SIS and INTERPOL's Stolen and Lost Travel Document database prior to entering the Schengen Area.[90] The European Commission informed the Task Force that evaluations are also conducted to ensure compliance with EU directives and that Member States are conducting systematic checks.[91]

Finally, EU states have not yet taken full advantage of PNR data to enhance their screening and vetting capabilities. PNR data can be analyzed to identify potential malicious or suspicious individuals who may require additional scrutiny based on their previous travel patterns or other biographical identifies and selectors. In early 2016, the EU issued a directive mandating Member States create Passenger Information Units (PIUs)—similar to CBP's National Targeting Center—that would be tasked with collecting, storing, and using PNR data to screen for terrorists and other criminals seeking to enter or transit through their countries. These PIUs will also be responsible for sharing PNR with other Member State PIUs, Europol, and in certain circumstances, third party nations.[92] The directive requires these PIUs to be established by mid-2018, although U.S. and European officials have expressed concern that not all Member States will be able to meet that deadline.[93]

Given the robust analytical capabilities of CBP and other U.S. government entities, and the success with which they have utilized PNR data to vet people looking to enter the United States, the U.S. government should offer to assist our EU partners in establishing their PIUs. In fact, the Task Force was heartened to learn that both the Belgian and Dutch governments have reached out to CBP for assistance and will likely have their PIUs established by mid-2018, if not sooner.[94] The Task Force encourages DHS to continue assisting our allies by sharing its experiences using PNR data.[95]

Europe's terror threats and counterterrorism capabilities directly impact the security of the U.S. homeland. A more secure Europe will help reduce the threat to the homeland. As such, helping our European allies enhance their counterterrorism capabilities is an investment in our own security.

Travel Document Security

Ensuring an individual's identity is vital when it comes to interdicting terrorists at ports of entry, as many potentially malicious actors have been discovered with altered or fake passports, papers belonging to siblings or relatives, or passports belonging to deceased individuals.[96] For example, in 2016, European border officials encountered more than 7,000 fraudulent documents at border crossing points to the EU from third party countries. In addition, over 11,000 fraudulent documents were encountered by border officials during crossings within the Schengen Area.[97] Further underscoring how serious this issue is, ISIS is known to have set up a fake passport "industry" from bases of operation in Syria, Iraq, and Libya, after acquiring a passport-printing machine.[98] It is important that our allies share accurate identity information with the United States so we can accurately confirm or resolve the identities of foreign nationals seeking the enter the United States.

The U.S. has pushed European partners to improve their technology to screen against identity fraud. As part of the VWP, the United States has required participating countries to issue their citizens fraud-resistant e-passports, similar to those issued by the United States.[99] E-passports are more secure because they are difficult to alter and include passenger biometric data, such as fingerprints, facial images, and iris scans. While meeting with European partners overseas, the Task Force was pleased to see that some partners are taking steps to enhance the security of their documents. The Belgian government, for example, is currently developing a risk analysis system for its passport, ID card, and foreign ID card issuance processes. They are also seeking to add facial recognition capabilities to Belgian passport issuance facilities, thereby allowing Belgian passport officials to use biometrics to confirm the identity of the passport applicant prior to issuing the document.[100]

Border Security Challenges

While checks at Europe's external borders have been strengthened, they are still not comprehensive enough to routinely detect terror suspects. Since 2015, close to 3 million asylum applications have been filed in EU countries, and as outlined earlier in this report, ISIS has already demonstrated the ability to exploit these flows to get operatives into Europe. For example, according to NCTC Director Rasmussen, "ISIS successfully sent several operatives—including at least two of the Paris attackers—from Syria to Western Europe by having them blend in with the flow of some 1 million migrants, asylum seekers, and refugees who traveled from Turkey to Greece in 2015."[101] Given the sustained battlefield defeats and the loss of its strongholds in Iraq and Syria, more foreign fighters may seek to exploit these same routes to return home. Therefore, it is vital that Europe expeditiously secures its borders and conducts robust screening on those seeking to enter in order to have situational awareness of who is on the continent.

Some of the border security issues are symptomatic of a larger, fundamental EU problem—diversity among Member States' income and productivity lead to imbalanced incentives in areas of shared responsibility. In this case, migrants come to Europe to live in wealthy Sweden or Germany, yet Greece and Italy are responsible for initiating border security measures for those and other European nations.[102] Thus, peripheral countries have an incentive to turn a blind eye to migrants and refugees as they do not want to bear future social or fiscal responsibility for them.[103] Part of the issue stems from the EU asylum process, known as the Dublin Convention. The law stipulates that the first country to fingerprint an asylum seeker—which should be the country of first entry—is then responsible for the individual's asylum claim

and the associated benefits.[104] This issue came to a head in late 2015, when the EU initiated legal action against Italy, Croatia, and Greece, which only collected 121,000 fingerprints of the 500,000 people who arrived in the second half of 2015, for failing to properly register arriving migrants.[105] The failure to collect these fingerprints is troubling, especially considering how valuable biometric information is for screening purposes and helping ensure terrorists or other malicious actors don't slip through the cracks when entering Europe.

Over the years, the European Union has taken a number of steps to bolster the security of its borders. In 2004, the EU founded Frontex, which was responsible for coordinating and enhancing cooperation among EU Member States with respect to managing the external borders of the EU. Throughout its history, however, Frontex suffered from myriad problems ranging from insufficient funds, staff, equipment, and cooperation with Member States, as well as a limited to non-existent coast guard. In order to help address some of the historical shortcomings of Frontex, the EU, in October 2016, reformed the agency into the European Border and Coast Guard Agency. The new agency will provide additional support to "hot spots" within the EU by conducting joint operations; collecting, analyzing, and disseminating information; and providing operational support to individual EU Members' border operations. According to the European Commission, there are plans to grow the organization from 300 to 1,000 full time employees by 2020.[106] Europol also recently created a "guest officer" program through which Europol members provide law enforcement officers and border security guards to support operational hotspots. These additional personnel, who are currently deployed in Greece and Italy, conduct additional security checks and assist with screening individuals seeking to enter the EU.[107]

There are other structural limitations within Europe that have prevented the borders from reaching optimal security. Per the Schengen Agreement, border checks are not required when travelling between Schengen countries. In the wake of the recent spate of attacks that have plagued Europe, several countries have instituted internal border checks. These checks, however, are temporary and can be waived in favor of the EU's freedom of movement principle in order to prevent long wait times at Schengen ports of entry.[108] Furthermore, the screening of individuals leaving the Schengen Area is extremely limited. As such, if malicious actors are not identified at their original point of entry into the Schengen Area, it is entirely possible for them to traverse, and possibly leave, the European Union with limited to no scrutiny, making it difficult for law enforcement and intelligence services to monitor them.

Under the European Union's freedom of movement principle, suspected terrorists can traverse numerous European countries in a matter of hours, creating major opportunities for terrorist exploitation.[109] The aftermath of two major European terror attacks demonstrates this potential vulnerability. Salah Abdeslam, a key figure in the November 2015 Paris attacks, managed to remain on the run for months, escaping from France and slipping easily into Belgium unnoticed.[110] Additionally, Anis Amri, who attacked a Berlin Christmas market in 2016, remained on the run for four days before being killed by Italian authorities in Milan, nearly 650 miles away.[111]

Legal Limitations

Due to a number of factors, including legal and policy challenges, European judicial systems have struggled to keep pace with the terrorist threat. According to a senior European official, in some European countries, there has been a reluctance to prosecute individuals for terrorism offenses, save for the most extreme cases.[112] European countries have struggled with collecting and gathering evidence that is admissible in court because military and intelligence-derived information is often excluded.[113] Given that a significant portion of the terrorists who have recently attacked Europe were on the radar of law enforcement, and in some cases, detained but later released, it is imperative European countries address the challenges in their judicial systems.

Recognizing that loopholes exist, most European parliaments are considering tougher, or have recently updated, counterterrorism laws to facilitate the prosecution of potential terrorists. Many of these changes were a result of the U.S.-led United Nations Security Council Resolution 2178, which requires UN members to prevent "the recruiting, organizing, training, or equipping" of foreign fighters.[114] In October 2015, the Council of Europe opened an Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism, which sought to criminalize participating in a group for the purpose of terrorism.[115] More recently, in February 2017, the EU Parliament approved a directive that criminalizes travel for the purpose of terrorism, terrorist training, funding terrorist activities, terrorist recruitment, public incitement or praise of terrorist acts, or aiding, abetting or attempting to execute a terrorist attack.[116] While Member States will have 18 months to adopt the legal changes outlined in this directive, U.S. officials overseas informed the Task Force that some countries have already made significant progress and are confident that other EU countries will meet the deadline.[117]

While the aforementioned legal and judicial issues are being sorted out, many European governments have turned to other administrative policies and options in the fight against terrorism. For example, the Dutch Ministry of Security and Justice can now use administrative measures such as travel bans and supervised check-ins to help keep tabs and mitigate the threat from potential terrorists in the country. In more extreme cases, Dutch authorities can even extend the length of pretrial detention when dealing with individuals accused of terror offenses. Meanwhile, according to Belgian officials, police now have expanded investigatory authorities and can use tactics that were previously not permissible, such as wiretaps and undercover stings, when dealing with terrorism. Belgian prosecutors have also expanded to use of witness protection programs and plea deals in order to bolster their ability to convict terror suspects.[118]

As part of the efforts to frustrate terrorist travel, several European countries now either confiscate the passports of their citizens who are known or suspected terrorists or make it otherwise impossible for these individuals to obtain travel documents. Belgium is a prime example, where officials informed the Task Force that they have placed 3,000 people on a "passport ban list," and have confiscated the national ID cards of 15 individuals due to terrorism concerns.[119] There has also been an increased focused on hate preachers and the role they play in the radicalization process. To counter their influence, European states have begun to more heavily scrutinize these sorts of individuals before letting them into the country. For example, in the Netherlands, hate preachers—both known and suspected—are subjected to special visa checks. According to Dutch officials, the Netherlands has also established local case management teams focused on containing radicalized individuals, preventing them from radicalizing additional people, and where possible, de-radicalizing them.[120] These programs and similar efforts will serve an important role for women and children returning from Iraq and Syria, who have been exposed to ISIS' ideology and violence and abhorrent conditions.[121]

The most drastic administrative measure European states have taken is the revocation of citizenship of known or suspected terrorists. It must be noted that only European citizens who are dual nationals have had their citizenship revoked. This measure is often utilized to prevent individuals who are currently in the conflict zone from returning to Europe. The extent to which citizenship revocation is utilized as a counterterrorism tool varies by country. On one hand, Belgian officials informed the Task Force that Belgium has only revoked the citizenship of four individuals, despite the Belgian Parliament recently passing a law that loosened the restrictions on revoking the Belgian nationality of terrorists.[122] On the other hand, in the United Kingdom, more than 150 people have been stripped of their British citizenship, including 30 between March and July of 2017 alone.[123]

With changes to their legal and judicial systems, European countries will be able to better address the terrorist threat. The February 2017 EU directive is a positive development and will help ensure European

states have more options for dealing not only with the threat currently emanating from the conflict zone but also with whatever threat emerges after the fall of the caliphate. As such, the Task Force encourages our European allies to take the necessary action in order to achieve compliance with the directive as quickly as possible.

U.S. CHALLENGES AND RECOMMENDATIONS

Underscoring the threat to the U.S. is the fact that terrorists have been able to exploit the visa system to enter the homeland. Hani Hanjour, one of the 9/11 hijackers, utilized a student visa to enter the country. Faisal Shahzad, who attempted to bomb Times Square in 2010, received a student visa and an H-1B visa. More recently, Tashfeen Malik, one of the terrorists behind the 2015 San Bernardino attack, entered the homeland on a K-1 fiancée visa.[124]

Despite the successes of our military on the battlefield and our law enforcement personnel at home, the United States continues to face one of the highest terror threat environments in the post-9/11 period. Acting Secretary of Homeland Security Elaine Duke outlined in November 2017 while testifying before the Committee, as the United States "takes the fight to groups such as ISIS and al-Qa'ida, we expect operatives to disperse and focus more heavily on external operations against the United States, our interests, and our allies."[125] This warning is underscored by the fact that since 2014, 45 people in the United States have been accused of being involved in plots to carry out attacks on U.S. soil.[126] There have also been seven ISIS-linked terror plots against the homeland thus far in 2017.[127] Finally, according to FBI Director Christopher Wray, there are currently "1,000 open ISIS-related investigations" in the United States.[128]

While tremendous progress has been made, we must work diligently to ensure that any outstanding vulnerabilities are addressed. Therefore, as a result of its investigation, the Task Force has seven recommendations designed to close gaps in our defenses. Given the nature of the threat, it is imperative that Congress and the Executive Branch work together to enact these recommendations expeditiously to help ensure the American homeland is as secure as possible.

Information Sharing

Challenge

As foreign terrorist fighters seek to return home or travel to other regions in the wake of ISIS' defeat on the battlefield, cooperation among U.S. military, national security, and law enforcement agencies and foreign partners is critical. One of the many challenges of fighting a dispersed, non-state actor is the ability to coordinate and unify the opposition effort. As foreign fighters move from Iraq and Syria back to the West, or to other regions, evidence collection and tracking becomes very difficult. An enhanced, whole-of-government effort to share information and intelligence related to these fighters and their movements will improve our security.

The United States must prioritize any opportunity to identity bad actors, including terrorists, outside the country and expand our ability to identify and deter threats before they reach the homeland. Unfortunately, information sharing challenges among U.S. agencies and with our foreign partners can prevent valuable information from becoming available for frontline screening and vetting in a timely manner. Not only is this a bureaucratic challenge—given the number of separate government agencies and components involved—but legal, capacity, and technical issues exist as well.

The key legal issues stem from the changing nature of the fighter, the type of derogatory information on that fighter, the entity that holds the information, and how that information was garnered. For example, if the U.S. military recovers intelligence in Mosul that an ISIS fighter has left Iraq for Europe, it will seek to get that information into the hands of U.S. national security entities, as well as relevant foreign partners.

It is not always as easy as pressing "send." The information collected may have a specific classification so other agencies may receive it in a very compartmentalized manner or may be prevented from receiving it at all. This issue is exacerbated when that information is needed to prosecute a potential terrorist in court, or when that individual is a U.S. person. Additionally, the revelation of the data itself may be enough to give away additional information or sources and methods that the U.S. government may not want revealed to foreign partners.

Even if these issues are properly addressed, capacity challenges can also be a major hindrance to sharing such information. The Task Force heard repeatedly that the volume of data being recovered in the combat zone is so large that it overwhelms our capacity. In addition to the sheer quantity of data, much of the information recovered must also be translated to English before it can be readily used. Ultimately, this can lead to a backlog of potentially valuable information on foreign fighters and other terrorists in the region, thus delaying the transfer of that data to DHS, the FBI, the State Department, and others.

Technical challenges can further hinder the timely passing of information and finished intelligence within and between agencies. In the above example, the derogatory information recovered in Iraq may be held in a Department of Defense (DOD) system, which may not automatically link to DHS or State Department systems. This could unnecessarily delay the sharing of data by requiring manual processing by analysts and increase the chances of someone slipping past our frontline screeners (though there has been some good progress in this area in recent years).

Furthermore, DHS uses its law enforcement authorities to work with a broad array of foreign partners on joint investigations outside the United States aimed to detect and interdict terrorists and criminals who may seek to exploit illicit migration routes to the homeland. Getting this information into the hands of frontline screeners and other law enforcement in the United States is just as important. Unfortunately, according to U.S. officials, technological, communication, and personnel challenges can impede the timely and efficient transfer of this data from the field back to the United States for processing, analysis, and translation—often causing significant delays in making this valuable information readily available to frontline DHS components and the broader U.S. interagency.[129]

The State Department, DHS, DOD, and other agencies have made great strides on biographic and biometric information sharing, but challenges remain. Currently, DHS receives biographic and biometric information from the Terrorist Screening Center (TSC), as well as DOD information collected in military theaters.[130] This allows DHS and the State Department to screen all encounters—including ESTA, visa applicants, refugees, and aslyees—against multiple biographic and biometric databases, vastly improving the ability to detect foreign fighters from the conflict zone.[131] However, as noted above, the sheer amount of data can overwhelm our agencies, especially those in the conflict zone.

Recommendation

These challenges can be overcome by allocating additional resources, which will help ensure faster analysis and transfer of collected data. Congress and the Executive Branch must address this challenge by providing additional funding, personnel, and technology—both in the field and in the United States—so that our agencies are able to collect information on the ground, analyze it appropriately, and send it out to relevant personnel and agencies. This will ensure that the derogatory information is getting into the hands of the frontline screeners and interviewers as soon as possible—increasing the chances of detecting and interdicting potential terrorists before they enter the homeland.

While additional resource allocation is the long-term solution to exploiting data from the field and maximizing its use across the U.S. government, there are short-term measures that the relevant agencies mentioned above can take and, indeed, are taking. In order to increase internal communication and information sharing, DHS personnel are currently embedded at numerous DOD locations domestically and abroad to evaluate information collected from conflict zones.[132] Additionally, the U.S. government has sought to formalize and expand partnerships within the interagency and with international partners. Perhaps the best example of this is Operation Gallant Phoenix (OGP), which Gen. Joe Dunford, Chairman of the Joint Chiefs of Staff, explained in June 2017 as furthering the "broad intelligence and information sharing network…established with the members of the anti-ISIS coalition."[133] He continued:

> A critical part of that effort is Operation Gallant Phoenix, an intelligence sharing arrangement that started out with eight or so countries, and has since expanded to 19 nations who have committed to sharing this intelligence. We're in the process of trying to expand that initiative to even more countries. Gallant Phoenix allows allied nations not only to share intelligence on the foreign fighter threat, but also to get that information back to their law enforcement and homeland security agencies so they have visibility on the movement of foreign fighters in order to deal with this challenge.[134]

While not a panacea for all information sharing gaps and challenges, OGP is a positive development for internal U.S. government—as well as international—coordination efforts between the military and law enforcement communities. After firsthand observation of OGP, the Task Force believes that it is a successful model that should be embraced and replicated. This critical effort has the ability to adapt in the ever-evolving fight against an unconventional enemy such as ISIS. However, fusion center models will not replace the need for additional resources for the military, DHS, and other agencies to take-in, process, and exploit valuable derogatory information.

Additional resources should also be prioritized for programs that further the collection of biometric and investigative data to inform visa screening—information that is critical to denying illicit travel. This includes support for ICE's BITMAP biometric collection and Transnational Criminal Investigation Unit (TCIUs), which play a critical role in pursuing national security related smuggling cases.[135] Furthermore, the success of such programs should not stop the U.S. government from continuing to seek and establish more permanent information sharing relationships and agreements with foreign partners.

Challenge

The U.S. government has a robust multilayered approach for screening and vetting foreign nationals who wish to enter the United States. As outlined earlier, this process involves several federal entities, mainly the State Department and DHS, along with other law enforcement and intelligence agencies. As the screening and vetting bureaucracy has grown over the years since 9/11, there is potential for unnecessary duplication, agency stove-piping, and gaps in the vetting infrastructure. Furthermore, it is imperative that agencies execute their Congressionally authorized responsibilities, along with their own internal policies and procedures, in order to avoid interagency turf battles and stove-piping that could limit information sharing and potentially allow a malicious actor to slip through the cracks.

Recommendation

CBP, ICE, the State Department, and other relevant entities should conduct a review of their current screening and vetting efforts to ensure that they are fully executing their statutory responsibilities, internal policies and procedures, and coordinating appropriately without any unnecessary duplication of efforts. Such a review should help identify and close gaps in the screening and vetting infrastructure and ensure the process is as robust and efficient as possible. If needed, the Executive Branch should work with Congress in an expedient manner to develop any required legislation to address the results of the review.

Screening and Vetting

Challenge

The visa application process presents a unique opportunity to assess travelers, enhance existing information, and identify previously unknown threats. However, since visa-issuing posts abroad often have limited law enforcement personnel and resources, they are not always able to conduct the best possible investigative work to improve such information. By fully taking advantage of the visa application process to conduct in-depth investigations of visa applicants where necessary, the United States could greatly enhance our counterterrorism information and ability to deny terrorists entry into America.

Currently, ICE coordinates the Visa Security Program (VSP), which deploys its HSI special agents to certain high-risk diplomatic posts worldwide to interdict terrorists and criminals seeking to exploit the visa process.[136] These agents provide advice and training to State Department consular officers based on specific security threats, review visa applications, and conduct additional investigations if warranted.[137] This program is a valuable tool for enhancing DHS screening and vetting of visa applicants, as well as for expanding DHS holdings and overall U.S. government information about individuals with ties to terrorism, or who should otherwise not be permitted to travel to the U.S. For example, in FY 2016, VSP and PATRIOT personnel recommended the refusal of 8,500 visas on various grounds, including terrorism, and were responsible for 1,669 TSDB nominations.[138] However, limited resources have slowed the development and expansion of the VSP to more posts and countries.

Recommendation

In order to enhance our vetting capabilities and capitalize on the visa application and interview process, DHS should seek to expand the VSP to additional high-risk posts. The expansion of additional VSP personnel around the globe will facilitate closer scrutiny of visa applications at consular posts that are determined to be at risk for the presence, activity, or transit of terrorists and criminals. Congress should prioritize additional funding for the VSP, and there should also be an exploration of alternative funding methods that could allow the program to expand more freely. Some, for example, have proposed the idea of a user fee as a solution that could alleviate the funding challenge by supplementing Congressional appropriations.

Where there are challenges stemming from the capacity of certain consular posts to accommodate VSP operations, the State Department and Congress should work with DHS to overcome such impediments. These challenges should not stand in the way of improving the security of the homeland. Additionally, if deploying additional VSP agents is determined not to be feasible at certain posts, then DHS should expand the use of personnel remotely performing the functions of VSP agents and the PATRIOT units supporting those agents.[139] This will provide some investigative analysis by ICE and maintain the screening and vetting efforts of PATRIOT analysts.

Challenge

Social media can provide a plethora of information that can be used for screening and vetting to identify known or suspected terrorists seeking to enter the United States. Social media information can be used to shed light on an individual's motives in ways biographic information simply cannot. In other words, it can be the red flag. However, many shortcomings prevent the wider use of social media vetting. This includes difficulty in identity resolution and creating consistent thresholding assessments for the determination of derogatory information. Greater use of social media information for screening and vetting purposes also requires increases in manpower and corresponding enhancements to training programs and technology.

Recommendation

Currently, ICE, CBP, and the State Department require certain visa applicants to provide the social media platform and handles they have used during the last five years, allowing them to search publically available information associated with those profiles. More should be done to leverage this growing mode of communication. The Executive Branch should consider expanding the use of information gathered from social media to screen and vet foreign nationals seeking to enter the U.S. ICE, for example, has developed an initiative that is designed to track the online activity of visa applicants, that are of particular concern, from the time of application through visa issuance and entry into the United States. (This recommendation reflects Committee passed legislation, H.R. 2626, the Strong Visa Integrity Secures America Act, which passed the Committee by voice vote on July 26th, 2017.)[140]

Working with the private sector, DHS should seek out new technologies that allow publicly available information collected from social media to be better incorporated into the screening and vetting process. Resources for the research, acquisition of the required technologies—specifically to achieve an automated capability—and training of personnel to support social media vetting is needed, and Congress and the Executive Branch must work together to address these resourcing needs. While it is reasonable to view social media simply as an additional selector, similar to a phone number or home address, there are privacy and civil liberties concerns that must also be considered given the amount of information associated with social media.

Challenge

The Terrorist Screening Center (TSC) is a multi-agency body staffed by contractors and temporary employees from DOJ, DHS, and State, responsible for maintaining the Terrorist Screening Database (TSDB). It was established in 2003 and is administered by the FBI. It does not have permanent statutory authorization. The TSC also facilitates information sharing and coordination among law enforcement, the intelligence community, and international agencies by offering one central point where all known terrorist-related information can be reviewed against the information of an encountered individual. Some have questioned that, today, the FBI, may not be the most appropriate entity to fulfill this mission, given that its institutional focus is on criminal and national security investigations and not border security, vetting, and screening. Given these challenges, ensuring appropriate coordination among the TSC, DHS, and other relevant agencies is imperative.

Recommendation

It is worth considering merging the TSC into CBP's National Targeting Center (NTC) since screening and vetting travelers is a logical extension of DHS' core border and aviation security mission. Furthermore, DHS is the largest consumer of TSDB information—CBP uses it to vet over a million travelers every day and the Transportation Security Administration (TSA) uses it to screen all aircraft passengers as well as transportation workers. Merging the TSC into DHS may also promote efficiencies within the screening and

vetting process. The Government Accountability Office (GAO) should assess the existing relationship between the TSC, DHS, FBI, and other relevant agencies, as well as make recommendations to Congress about what improvements may be necessary, including what entity is best suited to administer the TSC.

Challenge

Given the growing sophistication of our enemies, it is crucial our screening and vetting system is agile enough to best respond to emerging threats and trends. While there is a baseline for screening and vetting all foreign nationals seeking to come to the United States, these processes vary depending on several factors, including the applicant, visa category, and purpose of travel. Law enforcement and national security authorities currently conduct periodic threat-based assessments to determine the relative risk posed by each type of applicant—from non-immigrant visitors to immigrants to refugees. Furthermore, despite our robust screening and vetting process, sometimes derogatory information comes to light, or a person emerges as a threat, after being permitted to legally enter the United States. This may present a vulnerability since continuous screening of foreign nationals is not standard practice. Cases where derogatory information comes to light on a foreign national already in the United States are referred to ICE's Counterterrorism and Criminal Exploitation Unit (CTCEU), which is responsible for investigating visa violators who may pose a national security or public safety risk. It is imperative that DHS has the ability to identify and address all foreign nationals present in the U.S. who are determined, after their admission, to pose a threat to national security.

Recommendation

DHS should conduct a review of vetting standards for all foreign nationals seeking to enter or remain in the U.S. to ensure there are no missed opportunities to highlight any possible threats to our country. The review should also assess whether additional personnel or resources are necessary for DHS to identify and address situations where derogatory information comes to light after an individual enters the United States. DHS should build on existing CTCEU initiatives, such as the Visa Waiver Enforcement Program and the Recurrent Student Vetting Program, and expand the continuous screening of foreign nationals, in a risk based manner, to ensure it has to ability to address all foreign nationals who are determined to pose a threat to national security.[141] Furthermore, DHS should continue to examine their processes, technology, systems, and information sharing relationships to ensure they are the best possible for this crucial task. (This recommendation reflects Committee passed legislation, H.R. 2626, the Strong Visa Integrity Secures America Act, which passed the Committee by voice vote on July 26th, 2017.)[142]

Visa Waiver Program

Challenge

The Visa Waiver Program (VWP) requires partner nations to satisfy numerous security conditions in order to continue participation in this important program. Sharing of terrorist and criminal information is one such condition, pursuant to Homeland Security Presidential Directive–6 (HSPD-6) and Preventing and Combating Serious Crime (PCSC) agreements, respectively.[143] Despite signing these agreements with the United States, full implementation and reciprocal information sharing by some VWP participants is lacking.[144] VWP provides a unique opportunity for the federal government to encourage, and even require, our VWP partners to take additional security actions for continued participation in the program. While it may be difficult for some nations to meet these requirements, the United States must not fail to hold our partners accountable.

One potential way to enhance our security cooperation with VWP partners is to move towards formal, systematic, and continuous terrorist and criminal information sharing. While many VWP countries share

information with the U.S. through informal mechanisms and formal periodic exchanges of data, automated and continuous sharing yields the greatest benefit for both partners. For example, our systematic sharing with Canada "provides for nearly real-time access to visa and immigration data through [the] matching of fingerprints, as well as through biographic name checks for information that an applicant previously violated immigration laws, was denied a visa, or is a known or suspected terrorist."[145] While legal, technical, and resource challenges exist to mirroring this relationship with other nations, DHS and the State Department should leverage the strong relationship with Canada as a model for embracing and expanding systematic sharing with other trusted partners.[146]

Another potential area of improvement is biometric information sharing. ISIS and other Foreign Terrorist Organizations (FTOs) have significantly expanded their ability to obtain and use high-quality, fraudulent travel documents by utilizing criminal networks or internal capabilities. Some of the most valuable information collected by U.S. law enforcement or the military are biometrics. However, since there are a number of roadblocks (including capability, process, and policy challenges) to robust biometric information sharing, foreign fighters and other terrorists may be able to use assumed identities and fraudulent documents to avoid detection when crossing borders or encountering law enforcement in VWP countries.

Additionally, the bilateral nature of HSPD-6 and PCSC information sharing agreements between the United States and VWP nations limit the wider use of terrorist and criminal data. Thus, that information is not automatically making its way to countries—or critical international entities, such as Europol and INTERPOL—outside of the bilateral agreements. In addition, some VWP partners have been hesitant to exchange data, such as API and PNR, that can enhance screening and vetting operations. While the European Commission's adoption of the Passenger Name Record Directive is a positive step towards addressing this shortcoming, both the U.S. and our VWP partners can greatly benefit from a greater exchange of such important data.[147]

Lastly, despite the heightened threat, some of our VWP partners do not consistently use the information exchanged as part of the VWP to strengthen their own security. There are also VWP countries that lack the necessary resources and capabilities to integrate the analysis of API and PNR into their screening and vetting frameworks.

Recommendation

In light of the increasingly complex threat facing the homeland, DHS should continue to leverage the existing legal requirements of the Visa Waiver Program—namely those included in *Visa Waiver Program Improvement and Terrorist Travel Prevention Act of 2015* (Public Law 114-113)—to ensure our VWP partners are bolstering their capabilities and increasing their security cooperation with the United States. According to Acting Secretary Duke, DHS is already "pressing foreign countries to provide us more information on terrorists and criminals and … urging them to use the information our government already provides to catch global jihadists and other threat actors residing in or transiting their territory.[148] DHS should continue this engagement with our allies and, if necessary, transmit to Congress any enhancements to the VWP law that would support these goals.

Where feasible, the United States should expand the scope of terrorist identity information sharing with our VWP partners under HSPD-6 to include biometric data of KSTs, when available, and API and PNR data. Our allies should also increase their information sharing with important third-party entities like INTERPOL and Europol. Closer cooperation and greater information sharing will greatly enhance both U.S. and VWP country holdings regarding terrorists and foreign fighters.

DHS should encourage our VWP partners' domestic security services to incorporate the terrorist and criminal identity information exchanged via the VWP into their screening and vetting activities. Such

activities might include border inspections, aviation security, visa applications, and refugee and asylum processing. Finally, U.S. government entities, such has CBP, have been extremely successful in utilizing and analyzing PNR and API to identify and prevent individuals who may pose a threat to the homeland from entering the United States. Given this success, CBP should continue to proactively engage its European counterparts and offer assistance in helping them develop the capabilities needed to utilize advanced data as part of their screening and vetting apparatus.

APPENDICES

Appendix I: Task Force Activity

The list includes activities conducted by Members and/or staff of the Task Force; however, the listing is partial and does not include all activities, meetings, and other consultations conducted during the course of the Task Force's review.

Official Member Activities

Site Visit: The National Targeting Center and Terrorist Screening Center (March 2017)

Briefers: U.S. Customs and Border Protection, Federal Bureau of Investigation's Terrorist Screening Center

Briefing: Visa Security and the Visa Waiver Program (May 2017)

Briefers: Department of Homeland Security, U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement, Department of State

Hearing: "Denying Terrorists Entry to the United States: Examining Visa Security" (May 2017)

Witnesses: Department of Homeland Security, U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement, Department of State

Site Visit: The National Targeting Center and Terrorist Screening Center (June 2017)

Briefers: U.S. Customs and Border Protection, Federal Bureau of Investigation's Terrorist Screening Center

Briefing: National Targeting Center Programs (July 2017)

Briefers: U.S. Customs and Border Protection

Hearing: "The Terrorist Diaspora: After the Fall of the Caliphate"

Witnesses: The Foundation for Defense of Democracies, The Heritage Foundation, The RAND Corporation

Briefing: Terrorism in Europe and Threats to the United States (July 2017)

Briefers: Ambassadors to the United States from the European Union, France, and Germany

Site Visit: Dulles International Airport (September 2017)

Briefers: U.S. Customs and Border Protection

Official Staff Briefings

Department of Homeland Security

U.S. Immigration and Customs Enforcement

U.S. Customs and Border Protection

Office of Intelligence and Analysis

U.S. Citizenship and Immigration Services

INTERPOL Washington

Sandia National Laboratory

Official Task Force Travel

Jordan

U.S. Embassy

Department of Defense

U.S. Immigration and Customs Enforcement

U.S. Customs and Border Protection

Jordanian Directorate of Military Security

Belgium

U.S. Embassy (Tri-Mission: European Union, North Atlantic Treaty Organization, and Belgium)

European Commission Directorate General for Migration and Home Affairs

INTERPOL

NATO Counterterrorism Coordination Office

Belgian Ministry of Foreign Affairs

Belgian Ministry of the Interior

Belgian Ministry of Justice

Belgian Security Services (law enforcement and intelligence)

The Netherlands

U.S. Embassy

Europol

European Counterterrorism Center

Dutch Ministry of Security and Justice

The United Kingdom

U.S. Embassy

U.K. Home Office

MI5

Metropolitan Police

Other Task Force Meetings and Consultations

Members and staff also met with former government officials, think tanks, academics, professional organizations, and other individuals during the course of the review. Though they are not listed by name, the Task Force is grateful for the valuable input it received and the contributions of these individuals and organizations.

Appendix II: Abbreviations

ADIS – Arrival and Departure Information System

API – Advance Passenger Information

CBP – U.S. Customs and Border Protection

CIA – Central Intelligence Agency

DHS – Department of Homeland Security

CTCEU – Counterterrorism and Criminal Exploitation Unit

DOD – Department of Defense

DOJ – Department of Justice

ECTC – European Counter Terrorism Center

ESTA – Electronic System for Travel Authorization

ETAS- European Travel Authorization System

ETIAS – European Travel and Information Authorization System

EU – European Union

FBI - Federal Bureau of Investigation

FDNS – Fraud Detection and National Security Directorate

FTO – Foreign Terrorist Organizations

GAO – Government Accountability Office

GTAZ – Joint Counterterrorism Centre (German)

HSI – Homeland Security Investigations

HSPD – Homeland Security Presidential Directive

ICE – U.S. Immigration and Customs Enforcement

ISIS – Islamic State of Iraq and Syria

KST – Known and Suspected Terrorists

NCTC – National Counterterrorism Center

NTC – National Targeting Center

OGP – Operation Gallant Phoenix

PATRIOT – Pre-Adjudicated Threat Recognition and Intelligence Operations Team

PCSC – Preventing and Combating Serious Crime

PIU – Passenger Information Units

PNR – Passenger Name Record

SDF – Syrian Democratic Forces

SIS – Schengen Information System

TCIU – Transnational Criminal Investigation Unit

TIDE -Terrorist Identities DataMart Environment

TSA – Transportation Security Authority

TSC – Terrorist Screening Center

TSDB – Terrorist Screening Database

USCIS – U.S. Citizenship and Immigration Services

VSP- Visa Security Program

VSU – Visa Security Units

VWP – Visa Waiver Program

Appendix III: Endnotes

[1] More information on the Committee's previous Task Force can be found here: https://homeland.house.gov/press/committee-unveils-foreign-fighter-task-forces-final-report/.
[2] Thomas, Hegghammer, "The Rise of Muslim Foreign Fighters: Islam and the Globalization of Jihad, *International Security,* Vol. 35, *Winter 2010/11*, pg. 61.
[3] The Honorable Brett H. McGurk, Global Efforts to Defeat ISIS: Hearing Before the Senate Committee on Foreign Relations, 114th Cong., 2nd sess., June 28, 2016. *See also* "The European Union Terrorism Situation and Trend Report," Europol, 2017, https://www.europol.europa.eu/activities-services/main-reports/eu-terrorism-situation-and-trend-report-te-sat-2017.
[4] The Honorable John F. Kelly, Home and Away: DHS and the Threats to America: Remarks Delivered at George Washington University Center for Cyber and Homeland Security, https://www.dhs.gov/news/2017/04/18/home-and-away-dhs-and-threats-america.
[5] Yara Bayoumy, "Isis Urges More Attacks on Western 'Disbelievers'," The Independent, September 22, 2014, http://www.independent.co.uk/news/world/middle-east/isis-urges-more-attacks-on-western-disbelievers-9749512.html.
[6] Richard Barrett, "Beyond the Caliphate: Foreign Fighters and the Threat of Returnees," The Soufan Center, October 2017, http://thesoufancenter.org/wp-content/uploads/2017/10/Beyond-the-Caliphate-Foreign-Fighters-and-the-Threat-of-Returnees-TSC-Report-October-2017.pdf.

[8] The Department of State collects, on a mandatory basis, social media information from visa applicants who have been determined to warrant additional scrutiny in connection with terrorism, national security-related, or other ineligibilities. These applicants are required to provide social media platform and handles they have used during the last five years.
[9] The TSDB is colloquially referred to as the "terrorist watchlist" and is a central repository where law enforcement and other agencies can run a person-of-interest against U.S. government terrorism-related holdings.
[10] The National Targeting Center, which is run by the DHS component U.S. Customs and Border Protection, provides tactical targeting information aimed at interdicting terrorists, criminal actors, and contraband at the earliest point possible. It was authorized in P.L. 114-125.
[11] Executive Order No. 13781, 82 Fed. Reg. 50, March 13, 2017.
[12] The Honorable Brett H. McGurk, "Remarks at the Small Group Session of the Global Coalition to Defeat ISIS," November 15, 2017, https://www.state.gov/s/seci/2017remarks/275692.htm.
[13] "Country Reports on Terrorism 2016," U.S. Department of State, July 2017, https://www.state.gov/documents/organization/272488.pdf.
[14] These figures are based on open-source data compiled and analyzed by the Majority Staff of the Homeland Security Committee.
[15] "A timeline of the Islamic State's gains and losses in Iraq and Syria," Agence France-Presse, February 19, 2017, https://www.pri.org/stories/2017-02-19/timeline-islamic-states-gains-and-losses-iraq-and-syria.
[16] Peter Baker and Michael D. Shear, "Obama Says Strategy to Fight ISIS Will Succeed," New York Times, November 16, 2015, https://www.nytimes.com/2015/11/17/world/europe/obama-says-paris-attacks-have-stiffened-resolve-to-crush-isis.html.
[17] Anne Bernard and Hwaida Saad, "Raqqa, ISIS 'Capital,' Is Captured, U.S.-Backed Forces Say," October 17, 2017, https://www.nytimes.com/2017/10/17/world/middleeast/isis-syria-raqqa.html.
[18] Col. Ryan Dilion, U.S. Department of Defense, November 20, 2017, https://twitter.com/OIRSpox/status/932826704191676416.
[19] Colin Clarke, The Terrorist Diaspora: After the Fall of the Caliphate: Hearing Before the House Homeland Security Committee, 115th Cong., 1st sess., July 13, 2017.
[20] The Honorable John F. Kelly, "Home and Away: DHS and the Threats to America," Remarks Delivered at George Washington University Center for Cyber and Homeland Security, April 18, 2017, https://www.dhs.gov/news/2017/04/18/home-and-away-dhs-and-threats-america.
[21] The Honorable Daniel R. Coats, Worldwide Threat Assessment of the US Intelligence Community:

Hearing Before the Senate Select Committee on Intelligence, 115th Cong., 1st sess., May 11, 2017.
[22] Task Force Staff Delegation to The Hashemite Kingdom of Jordan, The Kingdom of Belgium, The Kingdom of the Netherlands, and the United Kingdom, August 2017.
[23] R. Kim Cragin, "The Challenge of Foreign Fighter Returnees," Journal of Contemporary Criminal Justice, Vol. 35, No. 3. *See also*: Robin Simcox, The Terrorist Diaspora: After the Fall of the Caliphate: Hearing Before the House Homeland Security Committee, 115th Cong., 1st sess., July 13, 2017.
[24] The Honorable Nicholas J. Rasmussen, World Wide Threats: Keeping America Secure in the New Age of Terror: Hearing Before the House Homeland Security Committee, 115th Cong., 1st sess., November 30, 2017.
[25] Rukmini Callimachi, K.K. Rebecca Lai, Karen Yourish, "ISIS Attacks Outside Its Self-Proclaimed Caliphate," New York Times, March 23, 2017, https://www.nytimes.com/interactive/2017/02/04/world/isis-remote-control-enabled-attack.html.
[26] R. Kim Cragin, "The November 2015 Paris Attacks: The Impact of Foreign Fighter Returnees," *Orbis*, Vol. 61, No. 2, 2017.
[27] The Honorable Nicholas J. Rasmussen, World Wide Threats: Keeping America Secure in the New Age of Terror: Hearing Before the House Homeland Security Committee, 115th Cong., 1st sess., November 30, 2017.
[28] *Ibid.*
[29] The Honorable Mike Pompeo, Remarks at Foundation for Defense of Democracies National Security Summit," October 19, 2017.
[30] The Honorable Nicholas J. Rasmussen, "CNAS Keynote Policy Address," May 3, 2017, https://www.dni.gov/files/NCTC/documents/news_documents/CNASopeningremarks.pdf.
[31] The Honorable Elaine C. Duke, Threats to the Homeland: Hearing Before the Committee on Homeland Security and Governmental Affairs, 115th Cong., 1st sess., September 27, 2017.
[32] R. Kim Cragin, "The November 2015 Paris Attacks: The Impact of Foreign Fighter Returnees," *Orbis*, Vol. 61, No. 2, 2017, pp. 212-226.
[33] The Honorable Mike Pompeo, Remarks at Foundation for Defense of Democracies National Security Summit," October 19, 2017.
[34] The Honorable Mike Pompeo, "Aspen Security Forum 2017: The View From Langley," July 20, 2017, https://aspensecurityforum.org/wp-content/uploads/2017/07/The-View-from-Langley.pdf.
[35] The Honorable Christopher A. Wray, World Wide Threats: Keeping America Secure in the New Age of Terror: Hearing Before the House Homeland Security Committee, 115th Cong., 1st sess., November 30, 2017.
[36] The George Washington University Project on Extremism, "GW Extremism Tracker: The Islamic State in America," November 2017, https://extremism.gwu.edu/sites/extremism.gwu.edu/files/Nov%202017%20Snapshot.pdf.
[37]House Homeland Security Committee, Majority Staff, Terror Threat Snapshot: September 2017, https://homeland.house.gov/wp-content/uploads/2017/09/09.08.17-Final-September-Terror-Threat-Snapshot-Report.pdf.
[38] "Defendant Charged with Conspiring And Attempting To Provide Material Support to ISIS," U.S. Department of Justice, August 31, 2017, https://www.justice.gov/usao-edny/pr/defendant-charged-conspiring-and-attempting-provide-material-support-isis.
[39] Nicole Chavez, Holly Yan, Eric Levenson, and Steve Almasy, "New York attack suspect charged with federal terrorism offenses," *CNN,* November 2, 2017, http://www.cnn.com/2017/11/01/us/new-york-attack/index.html.
[40] While the VWP was created in 1986, after 9/11 VWP travelers were required to obtain an Electronic System for Travel Authorization (ESTA) approval prior to traveling to the United States.
[41] National Commission on Terrorist Attacks upon the United States, The 9/11 Commission Report, Executive Summary, 2004. http://govinfo.library.unt.edu/911/report/911Report_Exec.pdf
[42] "TIDE Fact Sheet," National Counterterrorism Center, https://www.dni.gov/files/Tide_Fact_Sheet.pdf.
[43] Christopher M. Piehota, "Safeguarding Privacy and Civil Liberty While Keeping Our Skies Safe: Hearing Before the House Homeland Security Committee, 113th Cong., 2nd sess., September 18, 2014.
[44] Task Force Staff Delegation to The Hashemite Kingdom of Jordan, The Kingdom of Belgium, The Kingdom of the Netherlands, and the United Kingdom, August 2017.
[45] Edward J. Ramotowski, Denying Terrorists Entry To The United States: Examining Visa Security: Hearing Before the House Homeland Security Committee 115th Cong., 1st sess., May 3, 2017.
[46] Task Force Briefing with the Director of ICE's Visa Security Program, May 30, 2017.
[47] Michael Dougherty, John Wagner, and Clark E. Settles, Denying Terrorists Entry To The United

States: Examining Visa Security: Hearing Before the House Homeland Security Committee, 115th Cong., 1st sess., May 3, 2017.

[48] U.S. Government Accountability Office, Visa Waiver Program: DHS Should Take Steps to Ensure Timeliness of Information Needed to Protect U.S. National Security, GAO-16-498 (Washington, DC, 2016), https://www.gao.gov/assets/680/676948.pdf.

[49] API data includes travelers' biographic information primarily derived from the machine-readable zone of travel documents (such as passports) and PNR data includes information from an air carriers' reservation/departure control system.

[50] DHS Office of the Inspector General, DHS Tracking of Visa Overstays Is Hindered by Insufficient Technology, OIG-17-56, (Washington, DC, 2017), https://www.oig.dhs.gov/sites/default/files/assets/2017/OIG-17-56-May17_0.pdf.

[51] Michael Dougherty, John Wagner, and Clark E. Settles, Visa Overstays: A Gap in the Nation's Border Security: Hearing Before the House Homeland Security Committee, 115th Cong., 1st sess., May 23, 2017.

[52] Task Force Staff Delegation to The Hashemite Kingdom of Jordan, The Kingdom of Belgium, The Kingdom of the Netherlands, and the United Kingdom, August 2017.

[53] The Honorable Nicholas J. Rasmussen, Threats to the Homeland: Hearing Before the Senate Committee on Homeland Security and Governmental Affairs, 115th Cong., 1st sess., September 27, 2017.

[54] Task Force Staff Delegation to The Hashemite Kingdom of Jordan, The Kingdom of Belgium, The Kingdom of the Netherlands, and the United Kingdom, August 2017.

[55] *Ibid.*

[56] Sabrina Pabst, "From Hanover to IS: The case of Safia S", DW News, October 19, 2016, http://p.dw.com/p/2RRjc.

[57] *Ibid.*

[58] Jörg Diehl, Roman Lehberger, and Crhistoph Sydow, "Officials Lost Track of A Man Identified as Dangerous," Der Spiegel, December 22, 2016, http://www.spiegel.de/international/germany/attack-in-berlin-anis-amri-the-suspected-perpetrator-in-berlin-a-1127085.html.

[59] INTERPOL Purple Notices are used to transmit information on criminal methodology, objects, devices, and concealment methods.

[60] INTERPOL Blue Notices are used to share information about the identity, location, or activities of an individual related to a crime.

[61] Task Force Staff Delegation to The Hashemite Kingdom of Jordan, The Kingdom of Belgium, The Kingdom of the Netherlands, and the United Kingdom, August 2017.

[62] Julian E. Barnes and Stephen Fidler, "Brussels Attack Give New Impetus for More Intelligence-Sharing in Europe," The Wall Street Journal, April 18, 2016, https://www.wsj.com/articles/brussels-attacks-give-new-impetus-for-more-intelligence-sharing-in-europe-1460952001.

[63] House Committee on Homeland Security, Final Report of the Task Force on Combatting Terrorist and Foreign Fighter Travel, September 2015, https://homeland.house.gov/wp-content/uploads/2015/09/TaskForceFinalReport.pdf.

[64] The Schengen Agreement was the treaty that established the European Union's Schengen Area. The Schengen Area guarantees free movement between EU Member States without being subjected to checks when crossing internal borders.

[65] Jeff Seldin, "Europe's New Counterterror Center Unlikely to Make Quick Impact," VOA News, February 22, 2016, http://www.voanews.com/a/europe-new-counterterror-center-unlikely-to-make-quick-impact/3202101.html.

[66] Europol, The European Union Terrorism Situation and Trend Report 2017, June 2017, https://www.europol.europa.eu/activities-services/main-reports/eu-terrorism-situation-and-trend-report-te-sat-2017.

[67] Task Force Staff Delegation to The Hashemite Kingdom of Jordan, The Kingdom of Belgium, The Kingdom of the Netherlands, and the United Kingdom, August 2017.

[68] *Ibid.*

[69] Liz Alderman, "Terror Threats Thaw Budgets Across Europe," The New York Times, January 31, 2016, https://www.nytimes.com/2016/02/01/business/international/europe-training-financial-firepower-on-terrorism.html?_r=0.

[70] Task Force Staff Delegation to The Hashemite Kingdom of Jordan, The Kingdom of Belgium, The Kingdom of the Netherlands, and the United Kingdom, August 2017.

[71] Europol, The European Union Terrorism Situation and Trend Report 2017, June 2017, https://www.europol.europa.eu/activities-services/main-reports/eu-terrorism-situation-and-trend-report-te-sat-2017.

[72] Task Force Staff Delegation to The Hashemite Kingdom of Jordan, The Kingdom of Belgium, The

Kingdom of the Netherlands, and the United Kingdom, August 2017.

[73] Matthias Bartsch, et al., "Why did Germany Fail to Stop Terrorist?," Spiegel Online, January 5, 2017, http://www.spiegel.de/international/germany/germany-knew-terrorist-was-dangerous-but-failed-to-stop-him-a-1128423-2.html.

[74] "NYT: Refugees Pose Overwhelming Challenge to Europe's Police," Counter Jihad, October 25, 2016, https://counterjihad.com/nyt-refugees-pose-overwhelming-challenge-europes-police.

[75] Daniel Byman, "Frustrated Foreign Fighters," Lawfare, July 12, 2017, https://lawfareblog.com/frustrated-foreign-fighters.

[76] Rukmini Callimachi, "How a Secretive Branch of ISIS Built a Global Network of Killers," The New York Times, August 3, 2016, https://www.nytimes.com/2016/08/04/world/middleeast/isis-german-recruit-interview.html?_r=0.

[77] Daniel Byman, "Frustrated Foreign Fighters," Lawfare, July 12, 2017, https://lawfareblog.com/frustrated-foreign-fighters.

[78] Robin Simcox, "In Barcelona and Finland, Europe's New Normal," *Foreign Affairs*, August 2017.

[79] Allan Hall, "Germany's top spy warns the country faces 'massive danger' from 'brainwashed' ISIS women and children returning from Syria," The Daily Mail, December 3, 2017, http://www.dailymail.co.uk/news/article-5141149/Top-German-spy-warns-ISIS-women-children-returning.html.

[80] Task Force Staff Delegation to The Hashemite Kingdom of Jordan, The Kingdom of Belgium, The Kingdom of the Netherlands, and the United Kingdom, August 2017.

[81] Alissa de Carbonnel and Robert-Jan Bartunek, "Soldiers on Europe's streets dent NATO's defense edge", Reuters, September 14, 2017, https://www.reuters.com/article/us-europe-attacks-military-analysis/soldiers-on-europes-streets-dent-natos-defense-edge-idUSKCN1BP1CA.

[82] "German spy agency BND to get its own satellite", DW News, November 10, 2016, http://www.dw.com/en/german-spy-agency-bnd-to-get-its-own-satellite/a-36350903.

[83] Julian E. Barnes and Stephen Fidler, "Brussels Attack Give New Impetus for More Intelligence-Sharing in Europe", The Wall Street Journal, April 18, 2016, https://www.wsj.com/articles/brussels-attacks-give-new-impetus-for-more-intelligence-sharing-in-europe-1460952001.

[84] Europol, The European Union Terrorism Situation and Trend Report 2017, June 2017, https://www.europol.europa.eu/activities-services/main-reports/eu-terrorism-situation-and-trend-report-te-sat-2017. *See also*: Task Force Staff Delegation to The Hashemite Kingdom of Jordan, The Kingdom of Belgium, The Kingdom of the Netherlands, and the United Kingdom, August 2017.

[85] Richard Barrett, "Beyond the Caliphate: Foreign Fighters and the Threat of Returnees," The Soufan Center, October 2017, http://thesoufancenter.org/wp-content/uploads/2017/10/Beyond-the-Caliphate-Foreign-Fighters-and-the-Threat-of-Returnees-TSC-Report-October-2017.pdf.

[86] Task Force Staff Delegation to The Hashemite Kingdom of Jordan, The Kingdom of Belgium, The Kingdom of the Netherlands, and the United Kingdom, August 2017.

[87] *Ibid.*

[88] *Ibid.*

[89] *Ibid.*

[90] "Stopping foreign fighters at EU external borders," European Parliament News, February 16, 2017, http://www.europarl.europa.eu/news/en/press-room/20170210IPR61804/stopping-foreign-fighters-at-eu-external-borders.

[91] Task Force Staff Delegation to The Hashemite Kingdom of Jordan, The Kingdom of Belgium, The Kingdom of the Netherlands, and the United Kingdom, August 2017.

[92] "Commission Staff Working Document", European Commission, November 28, 2016, https://ec.europa.eu/transparency/regdoc/rep/10102/2016/EN/SWD-2016-426-F1-EN-MAIN.PDF.

[93] Task Force Staff Delegation to The Hashemite Kingdom of Jordan, The Kingdom of Belgium, The Kingdom of the Netherlands, and the United Kingdom, August 2017.

[94] *Ibid.*

[95] CBP officials informed the Task Force that CBP has participated in a number of EU-sponsored workshops on utilizing PNR.

[96] These figures are based on open-source data compiled and analyzed by the Majority Staff of the Homeland Security Committee.

[97] Frontex, Risk Analysis for 2017, February 2017, http://frontex.europa.eu/assets/Publications/Risk_Analysis/Annual_Risk_Analysis_2017.pdf.

[98] Brian Ross, Michele McPhee, and Lee Ferran, "ISIS Has a Whole Fake Passport 'Industry,' Official Says," January 25, 2016, http://abcnews.go.com/International/isis-fake-passport-industry-official/story?id=36505984.

[99] House Homeland Security Committee, Final Report of the Task Force on Combatting Terrorist and Foreign Fighter Travel, September 2015,

https://homeland.house.gov/wp-content/uploads/2015/09/TaskForceFinalReport.pdf.

[100] Task Force Staff Delegation to The Hashemite Kingdom of Jordan, The Kingdom of Belgium, The Kingdom of the Netherlands, and the United Kingdom, August 2017.

[101] The Honorable Nicholas J. Rasmussen, World Wide Threats: Keeping America Secure in the New Age of Terror: Hearing Before the House Homeland Security Committee, 115th Cong., 1st sess., November 30, 2017.

[102] European Commission, "The EU and the Refugee Crisis," European Union, 2016, http://publications.europa.eu/webpub/com/factsheets/refugee-crisis/en/.

[103] Michal Baranowski, Gordana Delic, Alexandra de Hopp Scheffer, Ian Lesser, Ozgur Unluhisarcikli, Ivan Vevoda, and Astrid Ziebarth, "The Refugee Crisis: Perspectives from Across Europe and the Atalntic," The German Marshall Fund of the United States, 2015, http://www.gmfus.org/publications/refugee-crisis-perspectives-across-europe-and-atlantic.

[104] Statement by the Council, the European Parliament and the Commission, "Regulation (EU) No 604/2013 of the European Parliament and of the Council of 26 June 2013," Official Journal of the European Union, 2013, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013R0604&from=EN.

[105] Corey Charlton, "EU starts legal action against Greece, Italy and Croatia for failing to fingerprint migrants: Tens of thousands have not been registered over last few months," Daily Mail, December 10, 2015, http://www.dailymail.co.uk/news/article-3354711/EU-starts-legal-action-against-Greece-Italy-Croatia-failing-fingerprint-migrants-Tens-thousands-not-registered-properly-months.html#ixzz4yKucpbsc.

[106] Task Force Staff Delegation to The Hashemite Kingdom of Jordan, The Kingdom of Belgium, The Kingdom of the Netherlands, and the United Kingdom, August 2017.

[107] *Ibid.*

[108] *Ibid.*

[109] According to Article 21 of the Treaty on the Functioning of the European Union, the freedom of movement principle allows EU citizens to freely move through and reside within the territory of all EU Member States.

[110] Steven Erlanger and Alissa Rubin, "Salah Abdeslam, Suspect in Paris Attacks, Is Captured in Brussels," The New York Times, March 18, 2016, https://www.nytimes.com/2016/03/19/world/europe/salah-abdeslam-belgium-apartment.html.

[111] Elisabetta Povoledo, Gaia Pianigiani, and Rukmini Callimachi, "Hunt for Berlin Suspect Ends in Gunfire on an Italian Plaza," The New York Times, December 23, 2016, https://www.nytimes.com/2016/12/23/world/europe/berlin-anis-amri-killed-milan.html.

[112] Task Force Staff Delegation to The Hashemite Kingdom of Jordan, The Kingdom of Belgium, The Kingdom of the Netherlands, and the United Kingdom, August 2017.

[113] *Ibid.*

[114] United Nations Security Council, "Resolution 2178 (2014), September 24, 2014, http://www.un.org/en/sc/ctc/docs/2015/SCR%202178_2014_EN.pdf.

[115] CETS No. 196, "Additional Protocol to Council of Europe Convention on the Prevention of Terrorism," Treaty Office, Council of Europe, October 22, 2015, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/217.

[116] Laura Agea, Caterina Chinnici, Cornelia Ernst, Lorenzo Fontana, Monika Hohlmeier, Petr Jezek, Eva Joly, and Timothy Kirkhope, "Preventing terrorism: clampdown on foreign fighters and lone wolves," European Parliament News, February 2, 2017, http://www.europarl.europa.eu/news/en/news-room/20170210IPR61803/preventing-terrorism-clampdown-on-foreign-fighters-and-lone-wolves.

[117] Task Force Staff Delegation to The Hashemite Kingdom of Jordan, The Kingdom of Belgium, The Kingdom of the Netherlands, and the United Kingdom, August 2017.

[118] *Ibid.*

[119] *Ibid.*

[120] *Ibid.*

[121] Allan Hall, "Germany's top spy warns the country faces 'massive danger' from 'brainwashed' ISIS women and children returning from Syria," The Daily Mail, December 3, 2017, http://www.dailymail.co.uk/news/article-5141149/Top-German-spy-warns-ISIS-women-children-returning.html.

[122] Task Force Staff Delegation to The Hashemite Kingdom of Jordan, The Kingdom of Belgium, The Kingdom of the Netherlands, and the United Kingdom, August 2017.

[123] "UK 'has stripped 150 jihadists and criminals of citizenship'," The Guardian, July 30, 2017, https://www.theguardian.com/uk-news/2017/jul/30/uk-has-stripped-150-jihadists-and-criminals-of-citizenship.

[124] Alex Nowratesh, "Terrorism and Immigration: A Risk Analysis," The CATO Institute: Policy Analysis No. 798, September 13, 2016.
[125] The Honorable Elaine C. Duke, World Wide Threats: Keeping America Secure in the New Age of Terror: Hearing Before the House Homeland Security Committee, 115th Cong., 1st sess., November 30, 2017.
[126] The George Washington University Project on Extremism, "GW Extremism Tracker: The Islamic State in America," November 2017, https://extremism.gwu.edu/sites/extremism.gwu.edu/files/Nov%202017%20Snapshot.pdf.
[127] House Homeland Security Committee, Majority Staff, Terror Threat Snapshot Data.
[128] The Honorable Christopher A. Wray, Threats to the Homeland: Hearing Before the Senate Committee on Homeland Security and Governmental Affairs, 115th Cong., 1st sess., September 27, 2017.
[129] Task Force Staff Delegation to The Hashemite Kingdom of Jordan, The Kingdom of Belgium, The Kingdom of the Netherlands, and the United Kingdom, August 2017.
[130] Department of Homeland Security Responses to Questions for the Record, House Committee on Homeland Security Hearing, "Denying Terrorists Entry to the United States: Examining Visa Security,"115th Congress, 1st sess., May 3, 2017.
[131] Department of State Responses to Questions for the Record, House Committee on Homeland Security Hearing, "Denying Terrorists Entry to the United States: Examining Visa Security,"115th Congress, 1st sess., May 3, 2017.
[132] Department of Homeland Security Responses to Questions for the Record, House Committee on Homeland Security Hearing, "Denying Terrorists Entry to the United States: Examining Visa Security,"115th Congress, 1st sess., May 3, 2017.
[133] James Kitfield, "CJCS Dunford Talks Turkey, Iran, Afghan Troop Numbers & Daesh," Breaking Defense, June 16, 2017, http://breakingdefense.com/2017/06/cjcs-dunford-talks-turkey-iran-afghan-troop-numbers-daesh/.
[134] *Ibid.*
[135] BITMAP is an ICE program that fills biometric databases with data collected from special interest aliens, violent criminals, fugitives and confirmed or suspected terrorists encountered within illicit pathways. This data helps form strategic pictures of the trends, networks and individuals connected with these pathways. TCIUs are ICE-led investigative units with members from foreign law enforcement agencies. *See also* https://www.ice.gov/international-operations.
[136] VSP agents are supported by the domestic-based Pre-Adjudicated Threat Recognition and Intelligence Operations Team (PATRIOT). *See also*: Department of Homeland Security, "Visa Security Program," U.S. Immigration and Customs Enforcement, February 23, 2016, https://www.ice.gov/visa-security-program.
[137] Department of Homeland Security, "Visa Security Program," U.S. Immigration and Customs Enforcement, February 23, 2016, https://www.ice.gov/visa-security-program.
[138] Michael Dougherty, John Wagner, and Clark E. Settles, Denying Terrorists Entry To The United States: Examining Visa Security: Hearing Before the House Homeland Security Committee, 115th Cong., 1st sess., May 3, 2017.
[139] PATRIOT is an interagency coordination effort to conduct advanced visa application vetting and enhance visa security that provides the ability to screen pre-adjudicated visa applicants against DHS holdings and uses ICE and CBP systems to return one overall DHS response regarding any potential concerns associated with visa applicant.
[140] The text of H.R. 2626 states, "…the Secretary shall, to the greatest extent practicable, and in a risk based manner and on an individualized basis, review the social media accounts of certain visa applicants…" The report for the bill states, "The Committee believes that screening visa applicant social media accounts will enhance the visa vetting capabilities of the U.S. Government both in the early stages of a visa application and at the issuance phase. It will allow for continued monitoring of high-risk non-immigrant visa holders during the time of visa application, issuance, and entry into the United States. This screening has the potential to identify additional derogatory information during the visa pre-issuance vetting phase which may otherwise be unknown."
[141] Michael Dougherty, John Wagner, and Clark E. Settles, Visa Overstays: A Gap in the Nation's Border Security: Hearing Before the House Homeland Security Committee, 115th Cong., 1st sess., May 23, 2017.
[142] The text of H.R. 2626 states, ''The Commissioner of U.S. Customs and Border Protection shall, in a risk based manner, continuously screen individuals issued any visa, and individuals who are nationals of a program country pursuant to section 217 of the Immigration and Nationality Act (8 U.S.C. 1187), who are present, or are expected to arrive within 30 days, in the United States, against the appropriate

criminal, national security, and terrorism databases maintained by the Federal Government.''

[143] HSPD-6 agreements are information sharing agreements utilized by the U.S. government to exchange terrorism information with foreign partners. PCSC agreements are information sharing agreements used to share information with foreign partners related to preventing, detecting, and investigation serious crimes.

[144] U.S. Government Accountability Office, Visa Waiver Program: DHS Should Take Steps to Ensure Timeliness of Information Needed to Protect U.S. National Security," GAO-16-498 (Washington, DC, 2016), https://www.gao.gov/assets/680/676948.pdf.

[145] Department of State Responses to Questions for the Record, House Committee on Homeland Security Hearing, "Denying Terrorists Entry to the United States: Examining Visa Security,"115th Congress, 1st sess., May 3, 2017.

[146] It should be noted that Canada is not one of the 38 VWP countries.

[147] Migration and Home Affairs, "Passenger Name Record (PNR)," European Commission, November 13, 2017, https://ec.europa.eu/home-affairs/what-we-do/policies/police-cooperation/information-exchange/pnr_en.

[148] The Honorable Elaine C. Duke, World Wide Threats: Keeping America Secure in the New Age of Terror: Hearing Before the House Homeland Security Committee, 115th Cong., 1st sess., November 30, 2017.

HOMELAND SECURITY
COMMITTEE