Chapter 15. Homeland Security

PULL QUOTE: "We continue to worry about international terrorism by groups like [al-Qa'ida] and ISIS, but now the threat from lone actors already here in the U.S. and inspired by those groups, the homegrown violent extremists, that threat is even more acute. . . . At the same time, we are particularly focused on domestic terrorism, especially racially or ethnically motivated violent extremists." – Christopher A. Wray, FBI Director[1]

Introduction of the Issue

In 1965, the first President's Commission on Law Enforcement and the Administration of Justice was focused on addressing the causes of crime and delinquency. Although radical violent organizations (e.g., the Ku Klux Klan) had long carried out campaigns of terror and groups (e.g., the Black Liberation Army and the Weather Underground) carried out violent attacks later in the 1960s and 1970s, the term "homeland security" was not yet part of the nation's vocabulary. It took the terrorist attacks of September 11, 2001, and the loss of thousands of American lives for law enforcement to focus their efforts on preventing and combating international and domestic terrorism. While there are varying definitions, the 2010 National Security Strategy defined homeland security as "a seamless coordination among federal, state, and local governments to prevent, protect against and respond to threats and natural disasters."[2]

In the nearly 20 years since 9/11, the threats that face the nation have expanded and diversified. Today, these threats come in many different forms, including foreign terrorist organizations (FTOs), radicalized lone actors, domestic violent extremists, malign influence campaigns by state and non-state actors, cyber and other threats to our national infrastructure, and the targeting of government institutions and national elections.

One of the key findings of the 9/11 Commission Report was that United States law enforcement and intelligence agencies needed to improve their ability to "connect the dots."[3] In the aftermath of 9/11, government agencies have made significant progress in breaking down information barriers, changing their culture, and being more transparent. Prior to 9/11, federal agencies shielded rather than shared their information. Now, that information is shared among the intelligence community (IC) and with other federal, state, local, tribal, and territorial law enforcement partners. In the past 20 years, the federal law enforcement community has developed ways to make information more accessible to key stakeholders by producing information at lower classification levels to reach a broader audience.

Another significant change since 2001 was the creation of the Department of Homeland Security (DHS) in 2002, which combined 22 different federal departments and agencies in a unified, integrated cabinet agency.[4] DHS's Office of Intelligence and Analysis equips the Homeland Security Enterprise with the intelligence and information needed to keep the nation safe, secure, and resilient. It also oversees the National Network of Fusion Centers that comprise 80 state and locally owned and operated fusions centers. One mechanism fusion centers use to share information is the Homeland Security Information Network (HSIN), which is DHS's official system for trusted sharing of Sensitive But Unclassified information between federal, state, local, territorial, tribal, international, and private sector partners. Mission operators use HSIN to access homeland security data, send requests securely between agencies, manage operations, coordinate

[1] Oversight of the Federal Bureau of Investigation (FBI), Before the House Judiciary Committee, 116th Congress (February 5, 2020) (verbal testimony of Christopher Wray, Director of the FBI).
[2] Office of the President. 2010. National Security Strategy of the United States: The White House, p. 2.
[3] National Commission on Terrorist Attacks upon the United States, The 9/11 Commission Report: Final Report of the National Commission On Terrorist Attacks Upon the United States. New York: Norton, 2004. Page 408.
[4] About DHS; History, accessed on www.dhs.gov on May 11, 2020.

safety and security for planned events, respond to incidents, and share the information they need to fulfill their missions and help keep their communities safe.[5]

The federal government made other significant changes to address homeland security after 9/11. The Federal Bureau of Investigation (FBI) shifted their priorities to counterterrorism, counterintelligence, and cyber security.[6] The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) created the role of the Director of National Intelligence (DNI) to serve as the head of the IC, which consists of 17 member agencies. The DNI leads the Office of the Director of National Intelligence (ODNI), another new cabinet level agency created post 9/11. The mission of the ODNI is to lead and support IC integration, deliver insights, drive capabilities, and invest in the future. The ODNI is staffed by officers from across the IC and is organized into directorates, centers, and oversight offices that support the DNI's role as head of the IC and manager of the National Intelligence Program (NIP).[7]

Information and intelligence are keys to enhanced coordination. While "homeland security" does not appear in the Johnson commission report, "intelligence" is mentioned 77 times. For example, "Procedures for the acquisition and channeling of intelligence must be established so that information is centralized and disseminated to those that need it."[8] While that sentence was written to address riots, it still pertains to threats the nation faces today and can easily be applied to terrorism and many other facets of homeland security. Notably, the biggest change in American law enforcement culture and organization over the past 50 years has been recognizing the importance of collaborating at all levels of government and with the communities they serve.

In an effort to advance the collective homeland security interests, the commission focused on three critical areas: identifying the nature of the threat, information-sharing and partnerships, and hardening vulnerabilities. The recommendations in this chapter are designed to enhance national security; maximize unity of effort across federal, state, local, tribal, and territorial entities; and protect the homeland for future generations.

This chapter focuses on recommendations made to keep the nation safe from terrorism, foreign threats, and other security concerns by strengthening laws, policies, funding, training, awareness, information-sharing, and partnerships to secure the nation against vulnerabilities from the Southwest Border to cybersecurity infrastructure and soft targets nationwide.

[BEGIN TEXT BOX]

Department of Homeland Security Today

"It is important to appreciate the great progress that the Department [DHS] has made since it was founded. DHS has adopted a multi-tiered approach to the lines of security we pursue, including aviation security and border security.

"By gaining the ability to recognize hostile actors long before they reach our borders, we have made our Nation's border's not our first line of defense, but one of many. We have increased the sharing of information about terrorist threats between the Federal Government and state, local, tribal, and territorial entities, as well as private sector partners. We have protected partners. We have protected America's critical infrastructure and empowered American communities. . . . But our work is not finished. Indeed, this is a pivotal moment in the Department's history, as we explicitly acknowledge, and adapt our tools to properly

[5] DHS website: https://www.dhs.gov/homeland-security-information-network-hsin accessed on May 11, 2020
[6] Director Robert S. Mueller, III, Before the House Appropriations Subcommittee on Science, the Departments of State, Justice and Commerce, and Related Agencies , Washington, DC , September 14, 2006.
[7] https://www.dni.gov/ accessed on May 13, 2020.
[8] Katzenbach, Nicholas, deB. U.S. President's Commission on Law Enforcement and The Administration of Justice, *Challenge of a Crime Free Society*, Washington: U.S Government Printing Office, 1967, p. 119.

confront, the threats of today. These threats have become more complex, more interconnected, more intertwined with technological advances, and closer to home. As the threats evolve, we must do so as well."

Kevin McAleenan, Acting Secretary, Department of Homeland Security *DHS Strategic Framework for Countering Terrorism and Targeted Violence, September 2019*

[END TEXT BOX]

15.1 Identifying the Nature of the Threat: International and Domestic Terrorism

Background

Nearly 20 years have passed since al-Qa'ida (AQ) operatives attacked the United States on 9/11. Terrorist organizations across the globe like AQ and the Islamic State of Iraq and ash-Sham (ISIS) continue to harbor the intent—and, in some cases, the capability—to harm Americans at home and abroad, despite having been broadly suppressed by counterterrorism operations throughout the Middle East and South Asia.

Equally concerning are their efforts to inspire homegrown violent extremists (HVEs)—mostly over the internet—to conduct terrorist attacks in the United States. This remains a concern for federal law enforcement agencies and their state and local partners. In addition to AQ and ISIS, foreign terrorist organizations use a range of political and terrorist tactics to undermine local governments, conduct attacks, and threaten American interests abroad.

Domestic violent extremists (DVE) in the United States today can be categorized as racially or ethnically motivated violent extremists (RMVE). This violent extremism covers several categories including anti-government/anti-authority, animal rights, environmental, and abortion-related. In 2019, DVE attacks in the United States resulted in the death of 32 individuals. This made 2019 the deadliest year in domestic terrorism since the 1995 bombing of the federal building in Oklahoma City that killed 168 individuals.

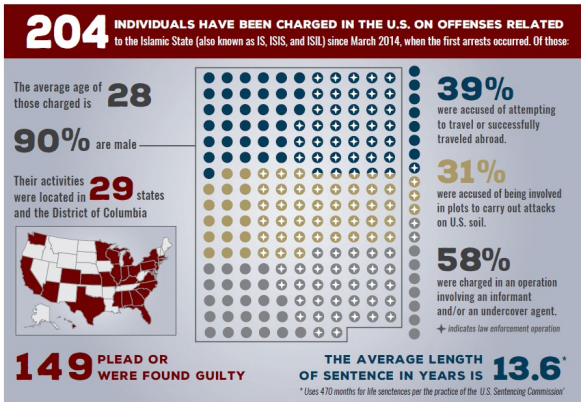
Lone actor violence within the United States has included attacks by violent extremists motivated by international and domestic terrorism. Homeland plotting, foreign travel, and the consumption of terrorist messaging by U.S.-based violent extremists inspired by foreign terrorist organizations has evolved significantly since 9/11. Homeland plotting has largely shifted from in-person networks motivated by local radicalizers to self-starting HVEs inspired by overseas ideologues, online radicalizers, and propaganda. Lone actor DVEs affiliated with domestic terrorist ideologies, particularly those associated with racially or ethnically motivated ideology, have become more prevalent, and their actions have become increasingly deadly.

HVEs continue to be inspired by a mix of ideological, sociopolitical, and personal factors. Most successful HVE attackers are radicalized during a period of one to four years and typically mobilized to violence in less than six months, suggesting there may be more time to detect plotters during the radicalization phase than the mobilization phase. In recent years, HVE plotters and attackers have trended younger, underscoring the susceptibility of some adolescents to violent extremist ideologies that appeal to their desire for belonging, identity, or attention. While ISIS continues to be a key influence, it is but one of several violent extremist influences that contribute to subjects' radicalization and mobilization. For example, now-deceased ideologue and AQAP senior leader Anwar Aulaqi continues to remain a key influence, more than nine years after his death.[9] Since 2014, there have been more than 200 people in the United States charged with offenses related

[9] Scott Shane, "The Enduring Influence of Anwar al-Awlaki in the Age of the Islamic State, CTC [Counterterrorism Center at West Point] July 2016, Volume 9, Issue 7. P. 15. https://www.ctc.usma.edu/the-enduring-influence-of-anwar-al-awlaki-in-the-age-of-the-islamic-state/

to ISIS.[10]

Like HVEs, DVEs continue to be inspired by a mix of ideological, sociopolitical, and personal factors that vary widely based on individual circumstances. Most drivers for DVEs include perceptions of government or law enforcement overreach, sociopolitical conditions, and reactions to legislation or world events. These trends are primarily enabled by the internet and social media that facilitates DVEs engaging with others without having to join organized groups. This online communication enables the sharing of literature promoting DVE beliefs which includes manifestos and ideologically-driven websites that contribute to DVE radicalization. More recently, DVEs are radicalizing based on personalized beliefs that do not correspond with a specific larger DVE threat, but rather a combination of views.



Source: Program on Extremism, The George Washington University, January 2020 Tracker.

Current State of the Issue

While combating terrorism and violent extremism is often associated with federal law enforcement agencies that lead the investigations, it is also a local and state problem. Local law enforcement tend to be the first responders such as the 9/11 attacks or the Boston Marathon bombing. In 2016, the Police Executive Research Forum recognized that "for police agencies and community members alike, violent extremism—which is ideologically motivated violence to further political goals—is a serious and immediate public safety concern." They published "Promising Practices for Using Community Policing to Prevent Violent Extremism" that offers recommendations for a whole-of-government approach that includes planning, training and community outreach and engagement.[11]

In his testimony before Congress, Christopher Wray, FBI Director, says that today, "The top threat we face from domestic violent extremists stems from those we now identify as Racially/Ethnically Motivated Violent Extremists (RMVE). RMVEs were the primary source of ideologically-motivated lethal incidents and violence in 2018 and 2019, and have been considered the most lethal of all domestic violent extremism movements since 2001."[12] RMVEs include a wide range of extremists including most notably those who advocate for the superiority of the white race. According to the New Jersey Office of Homeland Security and Preparedness, "white supremacist tactics indicate members are adopting strategies similar to those employed by foreign

[10] Seamus Hughes, Deputy Director, Program on Extremism, George Washington University, in discussion with the Homeland Security Working Group, April 6, 2020 and GW Extremism Tracker: The Islamic State in America accessed on June 11, 2020.
[11] Miller, Elizabeth and Jessica Toliver and David Schanzer. Promising Practices for Using Community Policing to Prevent Violent Extremism: How to Create and Implement and Outreach Plan." Police Executive Research Forum and Triangle Center on Terrorism and Homeland Security. Washington, DC, 2016, p. 3.
[12] Oversight of the Federal Bureau of Investigation (FBI), Before the House Judiciary Committee, 116th Congress (February 5, 2020) (written statement of Christopher Wray, Director of the FBI), P. 3.

terrorist organizations, including strict membership guidelines, online propaganda, and inspiring lone offenders. . . . In June 2018, a self-proclaimed white nationalist created a network called 'The Base,' which shares the English-language name for al-Qa'ida, to promote propaganda, [and] encourage violence against minorities."[13] Another extremist group is sovereign citizens. They are anti-government extremists who believe that even though they physically reside in this country, they are separate or "sovereign" from the United States. As a result, they believe they don't have to answer to any government authority, including courts, taxing entities, motor vehicle departments, or law enforcement.[14] According to the FBI, the greatest threat of violence against law enforcement by domestic extremists has emanated from those motivated by anti-government extremism, those acting against perceived threats to personal rights, and those acting against perceived unjust policing and judicial systems. Some form of this belief is common to several violent extremist ideologies, including sovereign citizen extremism and militia extremism. Anti-government extremists differ from these other categories in that they do not subscribe to these violent extremist ideologies in total but often adopt elements of these ideologies, including the use of violence in furtherance of their ideology.[15]

In recent years, lethal domestic terrorist attacks have been primarily perpetrated by lone DVEs or a few DVEs acting without a clear group affiliation or guidance. The current threat is driven by the spread and consumption of ideological content—often First Amendment-protected speech—which is then shared across online platforms by DVEs. DVEs also use these platforms to promote potentially radicalizing hate speech and post manifestos outlining grievances. Racial and ethnic minority groups, religious groups, law enforcement, and government personnel and facilities are often the primary targets. Most recent DVE attacks have been intended to inflict mass casualties against soft targets with easily acquired weapons—predominantly firearms. The law enforcement community continues to be challenged by the individualized nature of the radicalization and mobilization processes and the difficulty in distinguishing between violent rhetoric and actual terrorist intent. According to the FBI, out of 22 attacks with 79 fatalities from June 2015 to December 2019, racially or ethnically motivated violent extremists who advocated for the superiority of the white race were responsible for 11 of those attacks resulting in 52 fatalities.[16]

On the international front, despite enduring the loss of Usama bin Laden and other senior leaders, AQ's global network remains resilient. Its global affiliates continue to plan and carry out terrorist attacks against U.S. interests and allies overseas, while seeking new avenues to inspire or conduct attacks on U.S. soil. As American military deployments in historic AQ safe havens abate, the nation must find ways to enable foreign partners through capacity building and direct assistance. That, in turn, requires new strategies to collect intelligence on the group's plans and capabilities. These strategies will increasingly rely on strong collaboration with foreign partners, local law enforcement, and a more sophisticated understanding of how and where AQ operates online.

As with AQ, the focus on disrupting ISIS activities is becoming more dependent on the capacity building of and two-way sharing of intelligence with international partners. It also relies on cooperation among domestic and international law enforcement and private sector partners. The keys to preventing the group's

---

[13] New Jersey Office of Homeland Security and Preparedness Executive Intelligence Brief. "White Supremacist Extremists Exploit Jihadist Tactics." New Jersey Office of Homeland Security and Preparedness, December 16, 2019. https://www.njhomelandsecurity.gov/analysis/white-supremacist-extremists-exploit-jihadist-tactics accessed on June 4, 2020.

[14] Federal Bureau of Investigation, "Domestic Terrorism: The Sovereign Citizen Movement," April 13, 2010. https://archives.fbi.gov/archives/news/stories/2010/april/sovereigncitizens_041310/domestic-terrorism-the-sovereign-citizen-movement accessed on June 4, 2020.

[15] FBI, DHS and NCTC Joint Intelligence Bulletin, (U//FOUO) "Targeting of Law Enforcement by Domestic and Homegrown Violent Extremists." October 12, 2018.

[16] Federal Bureau of Investigation, "Counterterrorism Division Domestic Terrorism Threat Overview," April 2020.

resurgence and disrupting its actions are the collective partners' ability to disrupt ISIS's attempts to inspire or enable HVEs and other supporters in the United States and abroad.

As the threats to this country continue to evolve ranging from racially or ethnically motivated violent extremism (RMVE) and lone actors to cybersecurity and foreign threats, advances in technology have made it easier for adversaries to communicate and share information via social media and mobile devices. Unfortunately, law enforcement is hindered in its ability to leverage those tools for investigative purposes.

Many of these recommendations transcend both international and domestic terrorism threats. Implementing these recommendations will better position the federal government and its local, state, tribal, territorial, and private sector partners to prevent and mitigate threats of targeted violence.

15.1.1. **Congress should enact legislation that prohibits the provision or sale of data-storage devices or data-storage services that store data in such a way that the data is beyond the reach of a court-issued warrant.**

[CROSS REFERENCE TECHNOLOGY]

Law enforcement should have the ability to access electronic data and evidence to protect the public and to ensure homeland security. Criminals target individuals online by recruiting and radicalizing would-be terrorists on social media, stealing from online bank accounts, and selling drugs to children. Criminals also increasingly leave evidence of their plans and actions in exclusively electronic form, such as messages among co-conspirators. Law enforcement relies heavily on electronic information to counter every threat, from domestic and international terrorism to cyber intrusions, economic espionage, opioid trafficking, domestic abuse, and gang violence.

Strong encryption is necessary to protect our online lives. Increasingly, however, companies are building electronic devices and platforms that apply "warrant-proof" encryption, where those companies have designed their devices or systems to lock themselves out of data stored or transmitted so that they can no longer respond to court orders, such as lawful search warrants. Those companies are blinding the nation to preventable attacks, the identities and locations of sexually exploited children that could be rescued, and evidence against dangerous criminals that could be prosecuted.

Our nation should not have to choose between secure data and secure schools, neighborhoods, and streets; strong, responsible encryption gives us both. While it would be beneficial, law enforcement does not need to access providers' data directly as long as providers can access the data on their devices and platforms when ordered by a court to do so.

Elected officials should make the decisions that impact public safety rather than corporate officials whose fiduciary duty is to their shareholders. Lawful access requires a legal framework that protects privacy interests and civil liberties while also allowing investigators timely access to information to prevent acts of violence against persons or property. Lawful and timely access by investigators to evidence and other information is necessary to prevent terroristic acts, crimes of violence, and fraud, or to fully investigate such crimes after they have occurred. Thus far, corporations have been unable or unwilling to help craft a reasonable framework for lawful access to highly-encrypted or protected devices, services, and other media. Therefore, Congress should enact legislation that requires corporations to create lawful access capabilities for all consumer communications services and devices. All stakeholders should weigh in on appropriate changes to federal law to remove or re-balance the current immunities that corporate service providers have when they implement encryption tools that allow for otherwise preventable harms and injuries.

Domestic and international threat actors use platforms and devices that have end-to-end encryption to proliferate extremist content and motivate others to take violent action. As end-to-end encryption increasingly becomes embedded as a default in electronic devices and online peer-to-peer messaging applications, terrorists continue to exploit this technology to securely communicate and store information. These technological advances allow decentralized extremist groups to become more connected, resilient, and

capable. Today's aspiring terrorists need not meet their recruiters in person to join the group, be further influenced, or be tasked. Not unlike their exploitation of a free and democratic society, terrorists and extremists are openly exploiting rapidly evolving commercial platforms to offer more opportunities for self-radicalization and accelerate the speed of mobilization to violence. Commercially available encrypted tools are improving the operational effectiveness of designated terrorist organizations and radicalized lone offenders alike. Prospective terrorists and violent extremists use encryption largely available by default to facilitate offensive domestic operations and as an effective defensive tool, which prevents law enforcement from tracking their movements and intentions. Organic features of widely available social networking tools conveniently and effectively obscure networks, pre-operational planning, and global communication. In addition, full device encryption permits suspects to lock smartphones, tablets, computers, and other digital devices, which renders them almost entirely inaccessible. The globalization, sophistication, and casual availability of these capabilities is a growing challenge for law enforcement and national security efforts because they cannot legally access this information.

PULL QUOTE: "Thanks to the great work of the FBI—and no thanks to Apple—we were able to unlock Alshamrani's phones. The trove of information found on these phones has proven to be invaluable to this ongoing [Pensacola] investigation and critical to the security of the American people. However, if not for our FBI's ingenuity, some luck, and hours upon hours of time and resources, this information would have remained undiscovered. The bottom line: our national security cannot remain in the hands of big corporations who put dollars over lawful access and public safety. The time has come for a legislative solution."[17] - Attorney General William Barr

15.1.2 **Congress should enact legislation that ensures federal agencies have access to publicly posted data that is equal to the access provided to commercial entities.**

To efficiently search social media platforms for publicly available identifiers of suspected criminals, law enforcement entities use the same automated application programming interfaces (APIs) and access points that non-governmental entities routinely use for commercial and other purposes. These APIs allow law enforcement to perform automated searches across multiple platforms. When properly used, such tools help law enforcement conserve public resources and accelerate investigations, thereby enhancing their ability to identify criminals and bring them to justice.

Over the past few years, social media companies have added language to the terms of service that prohibit law enforcement from using APIs to develop tools to obtain information that is otherwise available to the public on their services. These companies have also added language that prohibits third parties from providing information obtained through the use of such APIs to law enforcement agencies. At the same time, these companies allow third parties to use their APIs to collect such information for other reasons, like monetizing the data and marketing goods and services.

Actions by social media companies in this environment reflect a growing trend. Social media companies, rather than elected officials, determine what information and technology law enforcement and public safety officials can use. In essence, decisions which have traditionally been made by elected officials are now being made by corporate officials. Law enforcement operates under the rule of law, abiding by the proper constraints and authorizations set forth by the Constitution and congressional action. The type of information law enforcement seeks is routinely provided to—and exploited by—others. Denying equal access to law enforcement authorities delays the time it takes to identify and stop criminal offenders. In many cases, while law enforcement is denied use of information made public by these companies, additional victimization occurs and the limited resources of law enforcement are expended. As a result, some victims may not be identified, and the perpetrators of the crimes against them may never be brought to justice.

The proposed legislation should preclude social media companies from excluding government agencies or

[17] William Barr, Attorney General, Pensacola Naval Air Station Attack Press Conference, May 18, 2020.

their agents from assembling, reviewing, and exploiting publicly-posted data if they allow other entities (e.g., marketers) to access and analyze data in such ways. With this access, law enforcement would be able to detect and prevent terrorism, radicalization, and other criminal acts of violence before they occur and without compromising privacy interests.

15.1.3 **The Department of Justice, the Department of Homeland Security, and the National Counterterrorism Center should produce an annual report for the public to increase awareness of terrorist threats and encourage public support.**

The public's understanding of the terrorism threat is increasingly integral to law enforcement efforts. Lone actors tend to select targets of opportunity or personal significance, which are difficult for law enforcement to identify and protect prior to an attack. This unpredictability in target selection reinforces the importance of threat awareness and education for not only law enforcement across federal, state, local, tribal, and territorial levels, but also for private sector partners and the public. In addition, law enforcement's ability to identify and disrupt lone actors has recently been impeded because law enforcement has not been able to access communications because of encryption. These limitations have increased the need for bystanders (e.g., family members, peers, community leaders, and strangers) to notice and report concerning changes in behavior before violence occurs. Regardless of whether law enforcement gains access to communications, it is better to have an informed public about potential threats and how they can help identify warning signs. The nation is stronger when law enforcement and an informed public work together.

15.1.4 **The Department of Justice, the Department of Homeland Security, and the National Counterterrorism Center should produce an annual terrorism threat assessment to better inform state, local, tribal, and territorial law enforcement officials of current threats.** .

The terrorism threat has significantly evolved since the attacks of 9/11. Known terrorists are now more likely to be homegrown, self-radicalized actors rather than formal members of FTOs. These homegrown violent extremists, together with racially or ethnically motivated violent extremists, pose a distinct threat to law enforcement because they are often lone actors with easily-acquirable weapons who attack soft targets.

The unpredictability in target selection, particularly regarding lone actors, reinforces the importance of threat awareness and education, especially for state, local, tribal, and territorial law enforcement authorities. An annual assessment would provide a look at how terrorism threats have morphed over the prior year and warnings for potential future threats.

The challenges facing the nation are significant. The Department of Justice (DOJ), the DHS, and the National Counterterrorism Center will continue to adapt ahead of evolving threats by implementing a whole-of-society approach that empowers its citizens; state, local, tribal, and territorial authorities; and private sector, non-governmental, and community leaders. It will also enhance the safety of the nation by producing an annual threat assessment that will help inform federal, state, local, tribal, and territorial law enforcement and private sector partners, and the broader public. A common baseline understanding of threats within the nation will support interagency policymaking, agency prioritizations, resource allocations, and inter-governmental partnerships.[18]

15.1.5 **The National Institute of Justice, in coordination with U.S. Probation and Pretrial Services, should research and develop best practices on supervising ex-inmates who were convicted of crimes relating to radical ideologies. These best practices should be disseminated to local, state, tribal, and territorial authorities.**

The National Institute of Justice, in partnership with U.S. Probation and Pretrial Services, should leverage

[18] Department of Homeland Security, Department of Homeland Security Strategic Framework for Countering Terrorism and Targeted Violence, p. 1 and 13. Note this recommendation complements the DHS Security Strategic Framework for Countering Terrorism and Targeted Violence's Objective 1.1: Conduct in-depth analysis of current and emerging threats, and share with the homeland security enterprise (p. 13).

their research, data, and experience to develop and share best practices for state authorities to supervise and monitor former inmates who served time for crimes related to radical ideologies or other charges, but who have known affiliations with radical ideologies. This special population needs tailored supervision to help ensure they do not inflict harm based on their radical beliefs. By leveraging research and disseminating best practices, local officials will be better informed and prepared if these individuals are released in their communities.

15.1.6 **State and local authorities should replicate the federal uniform prison release guidelines so state probation officers can better monitor inmates who have a connection to terrorism. These guidelines should include notification to the local Joint Terrorism Task Force and governors so they can notify their respective criminal justice authorities**.

Deputy Director Seamus Hughes raised a concern about the number of terrorist prisoners set to be released in the next 1.5 years He also noted that concerns about COVID-19 has led to the early release of prisoners. In the past, these prisoners who had been affiliated with terrorism would be released and travel to Syria and Iraq, but they cannot do that now based on travel restrictions.[19] Local, state, tribal, territorial, and federal law enforcement officials must strengthen the monitoring of released inmates who have a connection to terrorism.

Often, subjects of federal terrorism investigations are convicted of non-terrorism related charges. Others become radicalized in prison. Some domestic and international terrorist groups view detention and corrections populations as potential recruits. Unaffiliated extremist actors pose a similar threat, but they are often more difficult to detect as they may have self-radicalized and maintain no apparent terrorist affiliations. Some extremists attempt to influence inmates to join or support their cause while incarcerated or once they are released from custody through other extremist inmates, contractors, volunteers, or compromised staff.[20] Once released, these former inmates may pose as great a threat to the United States as those charged with providing material support to a designated FTO.[21]

The FBI and the Federal Bureau of Prisons jointly developed standard operating procedures to guide federal, state, local, and tribal authorities on how to monitor inmates charged with federal or state non-terrorism crimes who have a connection to international or domestic terrorism, in addition to those charged with federal terrorism charges. State and local authorities should notify the local Joint Terrorism Task Force (JTTFs) and governors when ex-inmates are released. The governors should then notify their criminal justice authorities and other key stakeholders so they are aware of newly released former inmates with potential terrorism ties.

15.1.7 **The White House should issue a National Security Presidential Memorandum aimed at strengthening and synchronizing terrorism and targeted-violence prevention programs across the nation.**

Recently there has been a recognition of the need to focus more on preventing terrorist and other targeted violence attacks, but no unifying guidance from the White House exists. As a result, state, local, tribal, and territorial law enforcement agencies are left to bridge prevention gaps on the fringes of their authority and resources. A national security presidential memorandum (NSPM) could provide the unifying guidance needed to strengthen and synchronize terrorism and targeted violence prevention efforts across the nation.

Congress recently provided $10 million in grants to support the development of prevention capabilities at the local level. Attorney General Barr directed the DOJ to implement national prevention and early engagement

[19] Seamus Hughes, Deputy Director, Program on Extremism, George Washington University, in discussion with the Homeland Security Working Group, April 6, 2020.
[20] Federal Bureau of Investigation, Identifying and Mitigating Extremist Activities in Corrections, p. 1.
[21] Richard Donoghue, U.S. Attorney for the Eastern District of New York, email communication with the Homeland Security Working Group Federal Program Manager, June 11, 2020.

programs across the nation. In addition, DHS established the Office for Targeted Violence and Terrorism Prevention. These efforts can support and complement a NSPM that provides much needed guidance to state, local, tribal, and territorial law enforcement agencies.

Over the past few years, the nation has endured numerous targeted violence attacks, many of which lacked any discernable ideological driver. According to the U.S. Secret Service, 27 mass attacks were carried out in public spaces in the United States in 2018, killing 91 people.[22] In 2017, 28 mass attacks claimed 147 lives, including the deadliest mass attack in modern history where 58 people were killed and injured 869 injured at an outdoor concert in Las Vegas.[23]

The solutions needed to proactively identify, assess, and prevent terrorist and other targeted violence attacks are similar; however, these solutions are applied disparately nationwide. In cases where ideological drivers are known or assumed, the FBI's JTTFs are involved. In cases where ideological drivers are not known or assumed, local law enforcement agencies with varying degrees of experience and capability may become involved. In some cases, no law enforcement agency will be involved until a crisis occurs. Such inconsistency impedes detection and assessment and decreases the likelihood of successful prevention exponentially.

Terrorism is just one form of targeted violence; having a NSPM that provides guidance to preventing such attacks whether it is a terrorist attack, mass shooting, or school violence would enable agencies to better thwart these types of attacks.[24]

15.1.8 **State, local, tribal, and territorial law enforcement agencies should designate officers as threat assessment and threat management coordinators and integrate them into threat assessment and threat management teams within their geographic area of responsibility.**

Highly effective multidisciplinary threat assessment and threat management (TATM) teams facilitate collaboration, coordination, and communication across organizations or communities to address persons of concern and threats of targeted violence ranging from terrorist attacks to school shootings. These TATM teams are often made up of a core group of representatives from relevant disciplines, such as law enforcement, security, mental health, social services, legal, human resources or administration, or others relevant to the agency establishing the team. A TATM team provides a versatile group of practitioners with different perspectives, capabilities, and backgrounds to address targeted violence concerns. Diverse perspectives can generate new investigative leads and prompt additional areas for inquiry, thus allowing for a more complete, holistic, and accurate threat assessment and management.[25]

Agencies across the country have applied the TATM team model to great effect. The Montgomery County Sheriff's Office of Dayton, Ohio, recently participated in a multidisciplinary TATM team hosted by the U.S. Marshals Service Southern District of Ohio and sponsored by the FBI's Behavioral Threat Assessment Center (BTAC). This multidisciplinary team reviewed a case involving a subject with a long history of threatening behavior rooted in perceived grievances against state and federal officials for more than a decade. The Montgomery County Sheriff's Office's multidisciplinary approach allowed the subject's family members to be

[22] United States Secret Service, National Threat Assessment Center, Mass Attacks in Public Spaces – 2018, July 2019.

[23] United States Secret Service, National Threat Assessment Center, Mass Attacks in Public Spaces – 2017, March 2018.

[24] If the White House issues an NSPM, it should fuse and leverage existing frameworks and guides such as Department of Homeland Security's *Strategic Framework for Countering Terrorism* and Targeted Violence; the Department of Justice's *Making Prevention a Reality: Identifying, Assessing, and Managing the Threat of Targeted Attacks;* the Criminal Intelligence Coordination Council's *National Criminal Intelligence Sharing Plan*, and the FBI's *National Information Strategy*.

[25] U.S. Department of Justice, Federal Bureau of Investigation, *Making Prevention a Reality: Identifying, Assessing, and Managing the Threat of Targeted Attacks, p. 70-71.*

involved and provided the subject much-needed assistance, which proactively prevented what could have ended in targeted violence.[26]

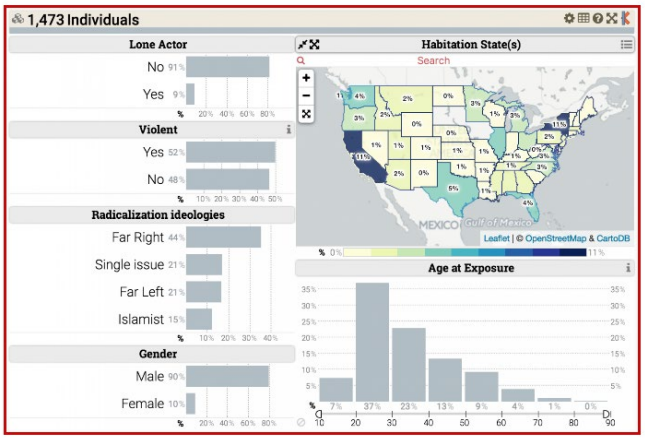
In another example, an FBI JTTF became aware of an individual radicalizing online. With the critical assistance from state and local partners, the subject was identified and the existence of a potential threat was confirmed, which included confirmation of an ISIS-inspired extremist ideology and operational capability. The multi-jurisdictional investigation also discovered the presence of mental health enhancers that potentially affected the subject's behavior and radicalization. The JTTF obtained the services of the FBI's BTAC to further assess the threat and to devise appropriate threat management strategies. Following a lengthy investigation and multiple consultations with the FBI's BTAC, threat management strategies were deployed and the investigation was resolved through local and federal prosecution, which resulted in enhanced locally mandated mental health assessment and services.[27]

While it is recommended that each state, local, tribal, and territorial, law enforcement agency have a TATM manager, many may not have the resources to dedicate to this effort. In those instances, it is recommended that local jurisdictions partner to identify a lead agency to serve as TATM. The return on investment is evident when potentially dangerous situations are prevented through proactive interventions led by the TATM.

15.1.9 **Congress should enact legislation that makes acts of domestic terror a violation of federal law.**

Currently, there is no specific federal statute that criminalizes acts of domestic terror. In the absence of such a statute, federal authorities must rely heavily on the use of local and state charges and are compelled to use substitute charges (e.g., civil rights, firearms, and weapons of mass destruction statutes) to prosecute defendants who have carried out domestic terror attacks. A statute modeled on already-existing statutes that criminalize foreign terrorist activities would provide an important weapon in the fight against domestic terrorism by aiding in investigative efforts, particularly against those who use the internet to radicalize online. This statute should also be crafted to ensure the protection of civil rights and civil liberties.

Profiles of Individuals Radicalized in the United States



Source: National Consortium for the Study of Terrorism and Responses to Terrorism[28]

[26] U.S. Marshals Service, Office of Protective Intelligence, January 2020.
[27] FBI Behavioral Analysis Unit-1, Behavioral Threat Assessment Center, April 2020.
[28] https://www.start.umd.edu/data-tools/profiles-individual-radicalization-united-states-pirus accessed May 8, 2020.

15.1.10 **Congress should enact legislation requiring state, local, tribal, and territorial law enforcement to report crimes relating to domestic terrorism incidents to the Federal Bureau of Investigation so that federal law enforcement can track and analyze domestic terrorist activity.**

According to the FBI, more U.S. arrests have been related to, and deaths caused by, domestic terrorist acts than international terrorism in recent years. However, mandatory reporting requirements of domestic terrorism incidents currently do not exist. As a result, it is difficult to identify changes in tactics and techniques or trends. Mandatory state and local reporting requirements would help identify trends throughout the United States. National Consortium for the Study of Terrorism and the Responses to Terrorism (START) Director Will Braniff testified before Congress that "defining, tracking, and reporting data on terrorism is subject to biases, subtle pressures or even manipulation. It's clear that domestic terrorism, specifically far-right extremism, requires greater attention and resource allocation."[29]

15.1.11 **State, local, tribal, and territorial law enforcement should voluntary track and share their domestic terrorism incidents with the Federal Bureau of Investigation.**

With no formal tracking requirements in place to gather data about domestic terrorism incidents from State, Local, Tribal, and Territorial law enforcement, the collection of domestic terrorism incidents should be added to information received from the more than 18,000 city, university and college, county, state, tribal, territorial and federal law enforcement agencies who voluntarily participate in the FBI's Unified Crime Report (UCR) program. The data should be submitted through a state UCR program or directly to the UCR program, and it should be included in the National Incident-Based Reporting System (NIBRS) beginning in 2021.

[CROSS REFERENCE DATA AND REPORTING]

15.1.12 **The Federal Bureau of Investigation should develop a public awareness strategy of domestic terrorism ideology and its relationship to hate crimes to help the public identify and report warning signs to prevent future attacks.**

In recent years, an increasing number of deaths have been caused by DVEs. The spate of attacks underscores the persistent threat posed by DVEs, including those who commit hate crimes to further DVE ideologies. To proactively address this threat from DVEs and to provide justice to those who are victims of hate crimes, the FBI established the Domestic Terrorism Hate Crimes (DT-HC) Fusion Cell in the spring of 2019.[30] Made up of subject matter experts from both the FBI's Criminal Investigative and Counterterrorism Divisions, the DT-HC Fusion Cell offers joint program coordination from FBI headquarters, which ensures an appropriate deployment of resources and seamless information sharing across divisions.[31] This joint perspective makes certain that law enforcement agencies are not solely focused on the current threat or the most recent attack, but are also looking to the future to mitigate this hybrid threat. As FBI Domestic Terrorism Analysis Unit Chief Debra Anderson said, "Messaging is something the FBI is concerned about. Some activity by [DVE] networks have been disrupted recently, but the COVID-19 pandemic may attract others towards accelerationism type goals, because the belief is political solutions will not work so they need to take action now."[32] Having a

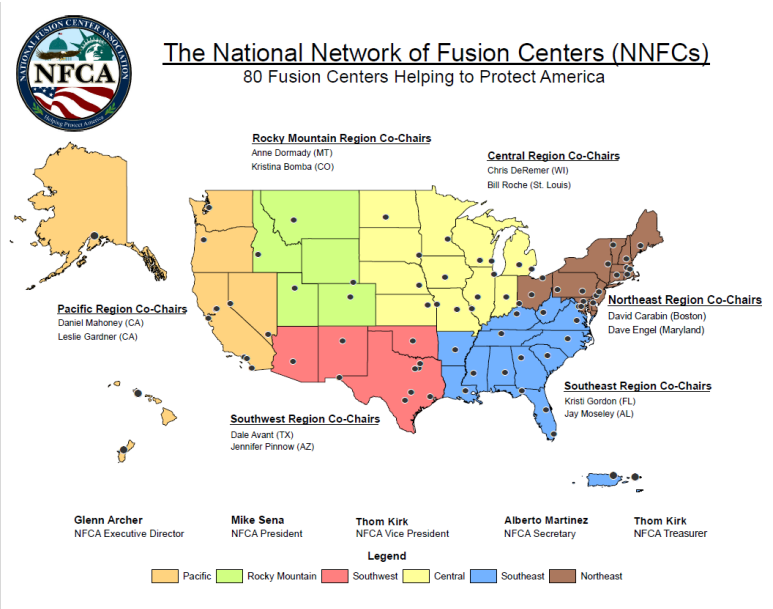
[29] William Braniff, director of UMD's National Consortium for the Study of Terrorism and the Responses to Terrorism (START), testified to the U.S. Senate Committee on Homeland Security and Governmental Affairs, September 25, 2019.

[30] Michael C. McGarrity, Assistant Director of Counterterrorism, FBI, Statement Before the House Oversight and Reform Committee, Subcommittee on Civil Rights and Civil Liberties, Washington, D.C., June 4, 2019. https://www.fbi.gov/news/testimony/confronting-white-supremacy accessed on May 14, 2020.

[31] Michael C. McGarrity, Assistant Director of Counterterrorism, FBI, Statement Before the House Oversight and Reform Committee, Subcommittee on Civil Rights and Civil Liberties, Washington, D.C., June 4, 2019. https://www.fbi.gov/news/testimony/confronting-white-supremacy accessed on May 14, 2020.

[32] Debra Anderson, Unit Chief, Domestic Terrorism Analysis Unit, Federal Bureau of Investigation, in discussion with the Homeland Security Working Group during the Identifying the Nature of the Threat meeting, April 6, 2020.

public awareness strategy can help inform the public of these emerging concerns.



Source: National Fusion Center Association

15.2 Information-Sharing and Partnerships

Background

Historically, law enforcement agencies have been hesitant to share information outside the confines of their own organizations. The 9/11 Commission Report highlighted this, noting, "The biggest impediment to all-source analysis—to a greater likelihood of connecting the dots—is human or systemic resistance to sharing information."[33] That hurdle no longer remains as a significant barrier. Since 9/11, law enforcement has dramatically changed how it operates. Federal, state, local, tribal, and territorial law enforcement agencies recognize they are stronger when working together. As a result, they have prioritized cultivating partnerships with each other, the private sector, and the community. These strengthened partnerships have led to more transparency and an increase in information sharing through such platforms as the FBI Law Enforcement Enterprise Portal and the DHS Homeland Security Information Network.

The federal government cannot connect the dots without the help of state, local, tribal, and territorial communities, and vice versa. The National Network of Fusion Centers (the Network) comprises 80 fusion centers across all states and territories that are owned and operated by state and local entities, with support from federal partners.[34] They facilitate two-way intelligence and information flow among the federal government, state, local, tribal, and territorial agencies, and private sector partners. Fusion centers conduct analysis and facilitate information sharing by assisting law enforcement, fire, public health, homeland security, emergency management, and private sector critical infrastructure partners in preventing, protecting against, and responding to crime and terrorism. The Network is a national asset that plays a critical role in enhancing the nation's ability to support public safety and counterterrorism missions. They also often assist

[33] National Commission on Terrorist Attacks upon the United States, The 9/11 Commission Report: Final Report of the National Commission On Terrorist Attacks Upon the United States. New York: Norton, 2004. Page 416.
[34] National Network of Fusion Centers Fact Sheet, Office of Intelligence and Analysis, Department of Homeland Security. https://www.dhs.gov/national-network-fusion-centers-fact-sheet .

in federal investigations.

On the private sector front, many entities have partnered with federal agencies to share critical data related to travel and global supply chains.[35] The FBI, DHS, and ODNI all established offices focused on partner engagement which work closely with state, local, tribal, and territorial law enforcement, fusion center partners across the country, and private sector partners.[36] DHS established the Public–Private Analytic Exchange Program that enables U.S. government analysts and private sector partners to gain a greater understanding of how their disparate, yet complementary, roles can operate in tandem to ensure mission success. Participants work to create unclassified joint analytic deliverables of interest to both the private sector and the federal government. This program focuses on such topics as cyber resilience and response, emerging technologies and national security, and vulnerabilities of health care IT systems.

Source: DHS Office of Intelligence and Analysis, Office of State and Local Partner Engagement

Current State of the Issue

Since the Johnson report, the United States has built a strong intelligence and information-sharing capability. That capability was enhanced considerably after 9/11, including establishing fusion centers, issuing security clearances to state, local, tribal, and territorial law enforcement personnel based on their roles and responsibilities as they relate to assisting the federal government in the fight against terrorism, accessing classified systems in state and local agencies, and declassifying information to make it accessible at the "law enforcement sensitive" or "for official use only" classification levels, therefore allowing critical information to reach a broader law enforcement audience. All these efforts have been focused on sharing knowledge and information with as many partners as possible, because such dissemination is vital to prevent and mitigate harm.[37]

[35] Roland Suliveras, Executive Director, National Targeting Center-Cargo, U.S. Customs and Border Protection, in discussion with the Homeland Security Working Group, April 27, 2020.
[36] Sarah Chervenak,FBI Unit Chief, Office of Partner Engagement and Russ Porter, Chief of Strategic Partnerships, National Counterintelligence and Security Center, Office of the Director of National Intelligence, in discussion with the Homeland Security Working Group, April 13 ,2020 and Alethea Madello, (A) Director, State and Local Partner Engagement, Office of Intelligence and Analysis, DHS and Susan Bower, State and Local Partner Engagement, Office of Intelligence and Analysis, DHS, in conversation with the Federal Program Manager, Amy Schapiro, May 1, 2020.
[37] Russ Porter, Chief of Strategic Partnerships, National Counterintelligence and Security Center,

While numerous partnerships have been cultivated, Assistant Director of National Intelligence Steven Mabeus is concerned that they are "generally personality-based, threat-related, and regional in scope."[38] Recognizing this as a potential weakness, many government agencies focus on institutionalizing sustainable partnerships rather than being dependent on individualized relationships. Examples include the global advisory committee, criminal intelligence coordination council, the homeland security advisory council, the national counterterrorism center's joint counterterrorism assessment team, and the DNI's homeland security and law enforcement partners board.

Law enforcement agencies at all levels of government have established robust partnerships with each other and other key stakeholders in the private sector, the community, and abroad. Still, more can be accomplished to connect the dots through partnerships and information sharing.

[BEGIN TEXT BOX]

Information Sharing

"Terrorism is terrorism. . . . We do not and cannot fight this battle alone. Our people are collaborating and communicating at a high level in Joint Terrorism Taskforces across the country and also within the numerous Fusion Centers throughout the nation.

In my career I have worked with many Fusion Centers to include some in your districts and the work we're doing together there is simply amazing. In fact, information provided by the Fusion Center in Orange County, California, led us to predicate cases that recently resulted in seven arrests of members of the base across four different states. Collectively, we are working around the clock to push out real-time intelligence to federal, state local, tribal, and territorial agencies.

This collaboration will continue to be vital as we face new trends in the threat."[39]

- Jill Sanborn, FBI Assistant Director of the Counterterrorism Division Testimony on Confronting the Rise of Anti-Semitic Domestic Terrorism, February 26, 2020

[END TEXT BOX]

15.2.1 **Federal, state, and local law enforcement agencies should better leverage, strengthen, and optimize existing intelligence or operational information fusion centers instead of creating new entities for law enforcement and interagency coordination. Such intelligence and information centers should continue to collaborate and promote nationwide interagency coordination and de-confliction.**

The best way to protect the nation is to leverage the existing—but distinct—intelligence, investigative, operational, and targeting entities that embody collaboration and expertise. No single agency can tackle the challenges and threats this country faces alone. By raising awareness about the National Network of Fusion Centers, the Drug Enforcement Administration's (DEA) Special Operations Division, DEA's El Paso Intelligence Center (EPIC), Customs and Border Protection's (CBP) National Targeting Center, the Organized Crime Drug Enforcement Task Force (OCDETF), and the High Intensity Drug Enforcement Areas (HIDTA) program and their specialties, law enforcement can maximize continued collaboration and partnership and prevent the unnecessary emergence of new entities.

Office of the Director of National Intelligence, telephone conversation with Amy Schapiro, Federal Program Manager, April 17, 2020.

[38] Steven Mabeus, Deputy Director of National Intelligence, Public Comment to the Homeland Security Working Group, April 30, 2020.

[39] Confronting the Rise of Anti-Semitic Domestic Terrorism-Part II, Before the Subcommittee on Intelligence and Counterterrorism House Committee on Homeland Security, U.S. House Of Representatives, 116th Congress (February 26, 2020) (written statement of Jill Sanborn, FBI Assistant Director of the Counter Terrorism Division).

15.2.2 **Congress should authorize and appropriate annual funding for the Department of Justice and the Department of Homeland Security to enable federal law enforcement agencies to establish full-time positions at all primary and recognized fusion centers that comprise the National Network of Fusion Centers.**

The National Network of Fusion Centers (the Network) represents a shared commitment between the federal government and the state and local governments that own and operate the fusion centers. Individually, each is a vital resource for collecting, analyzing, and integrating national, state, and local all-crimes, all-hazard information and making it relevant to their partners to prevent and respond to all threats and hazards. The Network provides critical investigative support to DOJ and DHS investigations by providing key local data and case support. Federal partners that assign personnel to fusion centers gain first-hand access to all of the established state and local relationships each fusion center has. They can also access local databases that they would not otherwise be able to access.

FBI Counterterrorism Assistant Director Jill Sanborn highlighted in testimony before Congress how one fusion center provided critical support to FBI investigations into seven individuals who were involved with racially motivated violent extremism.[40] Anecdotal evidence shows that fusion centers benefit from federal personnel being co-located at a fusion center. Director Chris Hayes and Deputy Director Alberto Martinez from the Orange County Information Assessment Center (OCIAC) both echoed the value of having federal employees, including those from the FBI and DHS, embedded in the OCIAC; this co-location is what makes the OCIAC strong.[41] According to the DHS's Office of Intelligence and Analysis in 2019, the FBI had approximately 90 personnel in 38 fusion centers and DHS had 95 personnel embedded in fusion centers.[42] However, the number of personnel is considerably less among other federal law enforcement agencies. The Bureau of Alcohol, Tobacco, Firearms, and Explosives has 12 employees working in fusion centers, and Immigration and Custom Enforcement (ICE) has 9 employees in fusion centers. The Drug Enforcement Administration, the Transportation Security Agency, Customs and Border Protection, and the Federal Law Enforcement Training Center all have either one or two representatives.[43]

The Network was established and evolved as a response to the 9/11 intelligence failures. Yet, without specific appropriated funding, federal law enforcement agencies have not been able to dedicate the needed personnel to make fusion centers even more robust. In 2016, based on a Congressional Directed Action (CDA) from the Senate Select Committee on Intelligence, the FBI was ordered to staff 70 positions at the National Counterterrorism Center.[44] The commission recommends congressional action to staff federal personnel at fusion centers. Fusion centers require the cooperative efforts of various member agencies to provide a mix of skills, experience, and enforcement jurisdiction which no single agency possesses. The Network's strength is its ability to draw upon the combined skills, expertise, and techniques of each participating agency, including federal law enforcement agencies.

[CROSS REFERENCE GRANTS]

---

[40] Confronting the Rise of Anti-Semitic Domestic Terrorism-Part II, Before the Subcommittee on Intelligence and Counterterrorism House Committee on Homeland Security, U.S. House Of Representatives, 116th Congress (February 26, 2020) (written statement of Jill Sanborn, FBI Assistant Director of the Counterterrorism Division).
[41] Chris Hayes (Director) and Alberto Martinez (Deputy Director), Orange County Intelligence Assessment Center), virtual site visit of the Orange County Intelligence Assessment Center, April 16, 2020.
[42] Rachel A. Seitz, Enterprise Performance and Evaluation, DHS I&A, email message to Amy Schapiro, Federal Program Manager, May 8, 2020.
[43] This data is based on the 2018 DHS I&A Fusion Center Cost Inventory, to be issued by the Department of Homeland Security, Office of Intelligence and Analysis.
[44] Jessica Davis, Counterterrorism Division, Federal Bureau of Investigation, email message to Amy Schapiro, Federal Program Manager, June 5, 2020.

15.2.4 **Congress should authorize and appropriate funding for a dedicated Department of Homeland Security fusion center grant program that provides funds directly to states and local jurisdictions that operate primary and recognized fusion centers comprising the National Network of Fusion Centers.**

[CROSS REFERENCE GRANTS]

The National Network of Fusion Centers brings critical context and value to homeland security and law enforcement partners. Fusion centers accomplish this through sharing information, providing partners with a unique perspective on threats to their state or locality, and being the primary conduit between frontline personnel, state and local leadership, and the rest of the homeland security enterprise. However, there is no dedicated funding program to sustain and support these ongoing collaboration and information-sharing efforts. Fusion centers receive operational funding from federal (both through grants and direct contributions), state, local, tribal, territorial, and private sector sources.[45]

Currently, most fusion centers receive funding through the Federal Emergency Management Agency Preparedness Grant Program, specifically the State Homeland Security Grant Program (SHSP) and the Urban Area Security Initiative (UASI). These funds represent varying percentages of overall fusion center budgets, with some centers mostly funded by state or local governments and other centers mostly funded through federal grants.

There is no certainty from one year to the next that a particular fusion center will receive funding that is adequate to build and sustain analytical, information sharing, and liaison capabilities to fulfill their missions and support local, state, and federal priorities. This uncertain support does not match the essential nature of the work that fusion centers perform. In addition, the current grant process pits law enforcement against emergency management and other state stakeholders for funding that is intended be focused on terrorism and violence prevention. As a result, consistent funding of critical prevention capabilities is not ensured. A dedicated fusion center grant stream would ensure that all primary and recognized fusion centers are able to plan, build, and maintain capabilities that are essential to their missions.

15.2.5 **The Department of Homeland Security should develop cross-jurisdiction online information-sharing training and education initiatives that promote teamwork, tactics, and technology to better equip an organization or region to implement both steady-state and crisis operations information-sharing capabilities.**

Personnel receive all types of training ranging from firearms to leadership, but there is little to no training available on how to best share information. An online training and technical assistance program should be developed that includes a tool kit on modeling how best to promote cross-jurisdiction information sharing with fusion centers, real-time crime centers, HIDTA, EPIC, DEA's Special Operations Division, CBP's National Targeting Center, the OCDETF, and the JTTF.

15.2.6 **The Department of Homeland Security and the Federal Bureau of Investigation should provide intelligence training to state and local authorities that focuses on integrating criminal intelligence with national intelligence to better protect the nation.**

The Johnson commission emphasized the importance of participation and coordination among federal, local, state, and private groups to address the problems at hand, and the sentiment has not changed in present time. In 1967, the focus was on organized crime and corruption.[46] Today, it is terrorism and security. What remains constant is the need to have informed leadership making critical decisions.

The Johnson commission recommended that enforcement officials provide regular briefings to leaders at all

[45] 2018 National Network of Fusion Centers Final Report, Department of Homeland Security, Office of Intelligence and Analysis, Page 4.

[46] Katzenbach, Nicholas, deB. U.S. President's Commission on Law Enforcement and The Administration of Justice, *Challenge of a Crime Free Society*, Washington: U.S Government Printing Office, p. 205 and 208.

levels of government concerning relevant conditions within each jurisdiction. The training proposed by this commission ensures that local leaders are briefed and understand the criminal and intelligence threat pictures.

By providing a fuller understanding through training of the information and intelligence landscape, state and local authorities are better positioned to understand potential threats that can have an impact on their decision making. This training should also provide an understanding of the capabilities of their local fusion centers.

15.2.7 **Congress should ensure grant funding to fusion centers and other law enforcement agencies for liaison officer programs. These programs should encompass a broad range of threats, including violent extremism, domestic terrorism, radicalization, cyber threats, and foreign threats.**

[Cross Reference Grants]

Terrorism and violent extremism from both internal and external actors is one of the most daunting domestic threats that affects the nation. Events that occurred in Oklahoma City, Oklahoma; Orlando, Florida; and San Bernardino, California, demonstrate the willingness of individuals to conduct attacks in our communities. One way to help prevent such attacks is to expand programs like the terrorism, intelligence, or fusion center liaison programs to train and leverage participants to recognize and report suspicious activity or potential threats. By expanding the threats that are incorporated into these liaison programs, there are more eyes and ears in the community. Liaison programs provide training for a diverse set of stakeholders, including establishing the central importance of privacy, civil rights, and civil liberties in recognizing and reporting suspicious or threatening behaviors.[47]

Many fusion centers have a liaison officer program including the Orange County Intelligence Assessment Center (OCIAC). In Orange County, California, they have 7,000 trained terrorism liaison officers (TLO) in 32 law enforcement agencies, 11 fire agencies, and many community sectors. Formal training is offered at the Orange County Sheriff's Academy and Orange County Fire Academy where there is access to new recruits.[48] These liaison officers are ambassadors from their home agencies to the OCIAC fusion center and vice versa. The focus of these TLOs is to drive information sharing from the ground up so everyone has good situational awareness. By adding more threats and funding to liaison officer programs, there will be significant return on investment as such programs serve as a force multiplier.[49]

15.2.8 **Federal, state, local, and tribal law enforcement organizations should leverage the existing Criminal Intelligence Coordinating Council to provide an ongoing solution to the need for a nationally coordinated, locally driven criminal intelligence sharing process.**

Regardless of the coordination that high-profile federal agencies work out among themselves, the Criminal Intelligence Coordinating Council (CICC)—a group formed post 9/11 under the DOJ's Global Justice Information Sharing Initiative (Global) that serves as an advisory body to the attorney general—supports and develops the capacity of all federal and non-federal agencies to generate and share criminal intelligence data. The CICC strives to ensure that every chief, sheriff, and law enforcement executive has a stake in its effort so that all law enforcement and homeland security agencies understand their role in the development and sharing of information and intelligence. The CICC also collaborates with federal partners to coordinate national initiatives focused on intelligence sharing. The advice and recommendations of the CICC and its

[47] Braden Schrag, Public Statement submitted to the President's Commission on Law Enforcement and the Administration of Justice, April 30, 2020.
[48] Nick Freeman (Captain) Orange County Fire Authority, virtual site visit of the Orange County Intelligence Assessment Center Virtual Field Visit, April 16, 2020.
[49] Nick Freeman (Captain) Orange County Fire Authority, virtual site visit of the Orange County Intelligence Assessment Center Virtual Field Visit, April 16, 2020.

membership have also been sought by the secretary of DHS, members of Congress, and representatives of state government. The CICC's mandate is to promote, ensure, and establish effective intelligence sharing and to address and solve the problems that inhibit this sharing.[50] To accomplish these tasks, the CICC must be central, permanent, and inclusive, and it must be staffed by law enforcement full-time personnel detailed from their respective local, state, tribal, and federal agencies

Because of its role within the nation's intelligence landscape, the CICC advises the attorney general, through the global advisory committee, on the best use of criminal intelligence to keep the country safe. The CICC also collaborates with federal partners—including the DOJ, the DHS, the FBI, the DNI, and the program manager for the information sharing environment—all in an effort to coordinate national initiatives focused on intelligence sharing.

The coordination produces the continued active involvement of local, state, and tribal law enforcement and homeland security agencies in nationwide criminal intelligence sharing efforts. It is only through the institutionalization of coordination and collaboration among all agencies—regardless of size and jurisdiction—that federal agencies can effectively and efficiently develop and share criminal intelligence.

15.2.9 **The Intelligence Community should develop a unified strategy to increase awareness of foreign influence threats that have an impact on state and local jurisdictions and the private sector.**

Today's complex counterintelligence threat requires a whole-of-society approach. Nation−state actors attempt to exploit America's economy, technology, information, and the rule of law, which threatens national and economic security. The law enforcement community is actively targeted by foreign adversaries seeking to compromise sensitive law enforcement information and databases and to influence law enforcement partners for malign purposes. Therefore, the federal government must raise awareness about these threats by sharing information and intelligence more widely. A particular focus should be on non-terrorist threats posed to homeland security, such as those advanced by well-financed, highly organized, and sophisticated foreign intelligence adversaries and their proxies who use social media and other platforms to drive division. The federal government should leverage the post-9/11 terrorism-related information-sharing structures and processes to broaden info sharing to include foreign intelligence threats, and to share relevant information with a wider range of recipients (e.g., governors, mayors, or heads of state, local, tribal, and territorial government entities). Organizational structures such as task forces established by the FBI must be prioritized.

Additionally, federal agencies should implement internal task forces to be similarly constructed to bridge agency responsibilities to reduce redundancy and better incorporate information sharing efforts that mitigate today's counterintelligence threat. The establishment of the FBI's Foreign Influence Task Force is an ideal standard by which the federal government can synthesize information, coordinate responses, and bring different authorities to mitigate threats. Organizational constructs such as task forces can be both permanent and ad-hoc to remain agile depending on the nature and scale of the counterintelligence threat.

15.2.10 The Bureau of Justice Assistance should fund the Criminal Intelligence Coordinating Council to provide a national assessment on progress in the integration of suspicious activity reporting capabilities in law enforcement computer-aided dispatch and records management systems.

A national assessment would identify implementation barriers, denote resource and technical challenges, and determine which additional resources are required to integrate computer-aided dispatch or records management system information into suspicious activity reporting (SAR) analysis and threat mitigation strategies. The Criminal Intelligence Coordinating Council, an advisory board to the attorney general, should lead and coordinate the national assessment.

15.2.11 The Department of Homeland Security should survey state, local, tribal, and territorial law

[50] https://it.ojp.gov/global/working-groups/cicc accessed on May 28, 2020.

enforcement, fire departments, and other emergency medical services information systems that may be used to improve reporting and analysis of threats of mass casualty attacks and threats to school safety. Special focus should be placed on information systems that can inform behavioral threat assessment processes and assist in the threat management process.

By surveying agencies to gather more knowledge about their information systems, the federal government can better leverage those systems to improve the reporting and analysis of mass casualty threats or school shootings. The federal government can also advance both the threat picture and the national suspicious activity reporting initiative by adapting existing processes, systems, and protocol.

15.3 Hardening Vulnerabilities

PULL QUOTE: "A secure border will lead to a more secure nation." - Sheriff Mark Napier, Pima County, Arizona[51]

Background

When discussing how best to strengthen the nation, the commission identified three vulnerabilities that threaten national security: border security, hardening soft targets, and cybersecurity.

The complex issues that border security entails have plagued the country for years. While much attention has been given to fortifying the Southwest Border, Sheriff Mark Napier of Pima County, Arizona, framed the issue in a broader content. He views border security as needing a three-tiered approach: addressing public safety, national security, and the human rights issue.[52] While acknowledging the lion's share of attention is focused on drug smuggling, gangs, sex trafficking, human smuggling, and illegal aliens, Sheriff Napier remains passionate that border security must be addressed as a humanitarian issue. He discussed the abuse many illegal aliens experience trying to cross the border coupled with the unforgiving environmental conditions at the border. He also discussed the financial and emotional toll on law enforcement to process, handle, and move decomposing bodies found in remote areas that are difficult to reach. Sheriff Leon Wilmot summed the state of the border best: "The lack of a secure border presents a public safety crisis, not only for border counties but also for our nation."[53]

In addition to the bleak picture painted by subject matter experts about border security shortcomings and the impact on national security; another area of concern was the safety and security of the public while attending large and crowded gathering places such as sports venues, night clubs, concerts, and movies. Such attacks have been seen in the United States from the Pulse Night Club massacre in Orlando and the Boston Marathon bombing to mass shootings at religious institutions of various denominations in Oak Creek, Wisconsin; Charleston, South Carolina; and Pittsburgh, Pennsylvania.

These places are considered soft targets and crowded places. This term is typically used to define locations or environments that are easily accessible, attract large numbers of people on a predictable or semi-predictable basis, and may be vulnerable to attacks using simple tactics and readily available weapons.[54]

---

[51] Mark Napier, Sheriff, Pima County (AZ) Sheriff's Department, in discussion with the Homeland Security Working Group, April 20, 2020

[52] Mark Napier, Sheriff, Pima County (AZ) Sheriff's Department, in discussion with the Homeland Security Working Group, April 20, 2020.

[53] Leon Wilmot, Sheriff, Yuma County (AZ) Sheriff's Office, Homeland Security Working Group Member, email communication to Amy Schapiro, Federal Program Manager, June 1, 2020.

[54] The Department of Homeland Security (DHS) Notice of Funding Opportunity (NOFO)
Fiscal Year (FY) 2020 Homeland Security Grant Program (HSGP), Page 3.

Jeff Miller, Vice-President of Security for the Kansas City Chiefs, spoke to the Commission about the multiple risks seen at such venues ranging from active shooters to critical infrastructure failures. Once these vulnerabilities and potential consequences are brought to the attention of decision-makers presiding over large venues, they often dedicate the needed funds for hardening their premises.[55] While Mr. Miller spoke in detail about safely securing sports stadiums, he pointed out the similarity of security and safety issues for other large, non-sports gatherings (e.g., parades) and the attendant vulnerability issues connected to them.

[BEGIN TEXT BOX]

Resources Available for Soft Targets and Crowded Places

The Department of Homeland Security (DHS) recognizes the need to raise awareness about the vulnerabilities inherent in soft targets and crowded places. In their Homeland Security Grant Program, administered by the Federal Emergency Management Agency (FEMA), one of their four prioritized areas includes, "enhancing the protection of soft targets/crowded places."[56] The FEMA grants available to local and state governments to support soft target preparedness activities are the State Homeland Security Program (SHSP) and the Urban Area Security Initiative (UASI). Information about both can be found here: https://www.fema.gov/homeland-security-grant-program

In addition to available funding, DHS has several resources available, including a guidebook about their efforts entitled *Soft Targets and Crowded Places Security Enhancement and Coordination Plan*, which other agencies can leverage to help protect soft targets and crowded places in their communities.

The DHS Office of Science and Technology published fact sheets, *Security for Large Crowds and Venues*[57] and *Predicting Crowd Behavior Fact Sheet and Video,*[58] which focus on enabling safer crowd movement during emergencies and other events.

[END TEXT BOX]

From each attack, new information is gleaned about how to prevent a repeat. For example, the Manchester, England, bombing at an Ariana Grande concert prompted the New York City Police Department (NYPD) to rethink how they secure major events. As NYPD Deputy Commissioner John Miller said, "The event does not end once everyone has entered safely. When people leave, the threat starts again."[59]

Another vulnerability the commission looked at was the need for heightened cybersecurity. As adversaries try to attack the security of this nation, they often attempt to infiltrate and harm cyber infrastructure which can have damaging effects on our critical infrastructure, democracy, and safety.

Current State of the Issue

As this commission report was being developed, the nation was confronted with a new threat: COVID-19. This pandemic has directly affected operations on the Southwest Border. In April 2020, the number of illegal migrant encounters at the Southwest Border were down 88 percent compared to the year prior.[60] Vehicular and pedestrian crossings were both down, largely because of travel restrictions implemented to slow the

[55] Jeff Miller, Vice-President of Security, Kansas City Chiefs, in discussion with the Homeland Security Working Group, April 27, 2020.
[56] The Department of Homeland Security (DHS) Notice of Funding Opportunity (NOFO) Fiscal Year (FY) 2020 Homeland Security Grant Program (HSGP), Page 3.
[57] https://www.dhs.gov/publication/st-security-large-crowds-and-venues-fact-sheet
[58] https://www.dhs.gov/publication/st-predicting-crowd-behavior-fact-sheet-and-video
[59] John Miller, Deputy Commissioner, NYPD, in discussion with the Homeland Security Working Group, April 27, 2020.
[60] (FOUO) CBP Weekly Messaging, Week of May 11, 2020.

spread of the coronavirus. During this time, narcotic seizures were up. [61]

Acting CBP Commissioner Mark Morgan said,

> Prior to being hit with COVID-19, each week, CBP encountered approximately 10,000 border crossers at the Southwest Border from dozens of countries. For the vast majority of those people, we don't know who they were, where they traveled, or what conditions they recently experienced. What we do know is that they don't have access to hand sanitizer and the human smugglers don't practice social distancing as they shove them into tractor trailers or overcrowded stash houses. From an infectious disease standpoint, what the smugglers put them through violates every aspect of what the medical experts say we must do to help stem the spread of this deadly disease.[62]

The national security threat the border represents is compounded by how it evolved since 9/11. The current concern is toward low-tech lone wolf type attacks, such as physical attacks with hand weapons in crowded areas, suicide bombings, and the weaponization of common vehicles. These single bad actors could easily enter the United States undetected through the southern border. We have ample evidence of the lethality that a single motivated person can possess through a very low-tech random attack. One of these people entering our country undetected is too many.[63]

In addition to the impact of COVID-19, there is concern about cyberattacks threatening the presidential election of 2020 and the ever present possibility of attacks on soft targets and in crowded places. Government officials have sounded the alarm about adversaries such as China leveraging their cyber capability to attack the United States. According to the DNI's World Threat Assessment, "Our adversaries and strategic competitors will increasingly use cyber capabilities—including cyber espionage, attack, and influence—to seek political, economic, and military advantage over the United States and its allies and partners. China, Russia, Iran, and North Korea increasingly use cyber operations to threaten both minds and machines in an expanding number of ways—to steal information, to influence our citizens, or to disrupt critical infrastructure."[64]

In Orange County, California, the Orange County Intelligence Assessment Center offers vulnerability assessments of critical infrastructure, including onsite physical threat assessments, and facilitates briefings with event personnel for mass gatherings. It also shares preventive awareness and DHS information. Recognizing the importance of vulnerability assessments, the OCIAC also provides training so these agencies can conduct physical threat assessments in the future.[65]

Border Security 15.3.1

15.3.1.1 **Congress should provide additional funding to federal agencies to construct and maintain a comprehensive border security system. This funding must support immigration enforcement detention capacity and space, technological infrastructure, and combined durable physical and technology systems that help secure national borders.**

One of the United States' greatest homeland security vulnerabilities is the lack of comprehensive border

[61] (FOUO) CBP Weekly Messaging, Week of May 11, 2020.
[62] Acting Commissioner Mark Morgan, Customs and Border Protection, "March Border Enforcement Results," WebEx Press Conference, May 7, 2020.
[63] Leon Wilmot, Sheriff, Yuma County Sheriff's Office, email communication to Amy Schapiro, Federal Program Manager, June 1, 2020.
[64] Coats, Daniel R., Director of National Intelligence. "Statement for the Record World Threat Assessment of the U.S. Intelligence Community", Senate Select Committee on Intelligence, January 29, 2019, page 5. https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf
[65] Greg Fox, Captain, Anaheim Fire and Rescue, in discussion with the Homeland Security Working Group during the virtual field visit to the Orange County Intelligence Assessment Center, April 16, 2020.

security. A secure border requires a layered approach that involves multiple stakeholders at federal, state, and local levels; technology; and durable combined physical and technology systems. These systems should include physical barriers where appropriate, sensors, and a fleet of surveillance drones that cover the entire U.S.−Mexico border. These drones would allow authorities to see in real time who and what attempts to cross the border. To properly manage and secure the border, there must be sufficient immigration enforcement detention capacity to effect the apprehension, detention, and subsequent removal of individuals who enter the United States illegally. These combined tools will provide adequate controls to manage and mitigate illegal migration flows, which will therefore improve national security and the safety of the American people.

15.3.1.2 **Congress should enact legislation that raises the penalty for illegally entering the United States from a misdemeanor to a felony. This legislation should also clearly state that being in the United States without legal authorization is a continuing offense, and that the statute of limitations does not begin from the time the alien illegally entered the United States.**

At present, illegally entering the United States is punishable only as misdemeanor (8 U.S.C. § 1325) which applies to asylum seekers but not if they come through a port of entry. This does not sufficiently deter those who are determined to enter the United States illegally, nor does it provide sufficient punishment for those who do. Further, when aliens are found in the United States more than a year after their illegal entry, criminal prosecution may be impossible if courts determine that the one-year statute of limitations began upon the alien's illegal entry.

15.3.1,3 **Congress should enact legislation to codify the authority of state and local law enforcement agencies to briefly maintain custody of prisoners and inmates for whom there is reason to believe they are aliens who could be removable from the United States. These inmates should be delivered to Immigration and Customs Enforcement's custody to face immigration removal procedures after serving their state sentence**.

State and local law enforcement partners who are willing to briefly detain alien prisoners and inmates so that ICE can take custody of them face legal jeopardy in some jurisdictions. Implementing this recommendation would lessen the litigation risks that are associated with cooperating with ICE and help secure the nation, as criminal aliens and terrorists who are removable from the United States will be removed according to established immigration laws and procedures.

15.3.1,4 **Congress should enact legislation that authorizes and appropriates the Federal Emergency Management Agency's Operation Stonegarden grant program to provide increased funding for border operations and resources geared for law enforcement agencies along the national border.**

[CROSS-REFERENCE GRANTS]

FEMA administers Operation Stonegarden (OPSG), a grant program that supports enhanced cooperation and coordination among CBP, United States Border Patrol (USBP), and federal, state, local, tribal, and territorial law enforcement agencies. The OPSG program funds investments in joint efforts to secure the United States borders along routes of ingress from international borders to include travel corridors in states bordering Mexico and Canada and in states and territories that border international water.[66] As the issues that plague the border intensify, particularly along the Southwest Border, law enforcement agencies along the nation's border need increased funding and resources to support operations. Dedicating the appropriated funding for Operation Stonegarden would enable a whole-of-community, counter network to defeat transnational criminal organizations and provide front-line anti-terrorism defense of the nation.

15.3.1,5 **Congress should authorize and appropriate funds to the Department of Justice to establish a grant**

[66] FEMA Grant Details, Operation Stonegarden, accessed on May 10, 2020 https://www.homelandsecuritygrants.info/grantdetails.aspx?gid=21875

program tailored to the Southwest Border. This program should address the public safety, national security, and humanitarian issues that are prevalent in border communities. This funding should go directly to local law enforcement agencies and not through the state authorities for dissemination.

[CROSS REFERENCE GRANTS]

Local law enforcement agencies along the Southwest Border are confronted with challenges unique to their jurisdiction. While their duties focus on protecting and serving the public, there are not many other agencies that confront the same volume of humanitarian issues, which include human smuggling, human trafficking, sex abuse, criminal abuse, transnational criminal organizations, or drug smuggling.

In addition, sheriffs on the Southwest Border house illegal aliens charged with state crimes. In Arizona, this leads to approximately $30 million every year in unanticipated costs for housing, feeding, and providing medical care to illegal aliens.[67] Through the Bureau of Justice Assistance's State Criminal Alien Assistant grant program, in partnership with ICE, local agencies are reimbursed for incarcerating undocumented criminal aliens with at least one felony and two misdemeanor convictions for violations of state or local law, and incarcerated with for at least four consecutive days during the reporting period.[68] Yet, border sheriffs say this is not enough and that the aid provided is equivalent to roughly five cents on the dollar for their expenditures, which does not begin to cover their incurred expenses.[69]

While grants are currently available to agencies along the Southwest Border, most funding is disseminated through the state and funneled down to local law enforcement. Administering grants directly to these local law enforcement agencies on the Southwest Border will reduce administrative costs and help streamline the grant-making process while providing needed funds to address the mounting humanitarian, public safety, and national security issues that law enforcement on the Southwest Border encounter daily.

15.3.1.6 **The legislative and executive branches should institutionalize a formal mechanism to ensure that border sheriffs and other key local stakeholders help formulate policy decisions that have an impact on the Southwest Border.**

Border sheriffs and other key officials and stakeholders who are involved in formulating their own policy decisions that have an impact on the Southwest Border know their territory and its inhabitants well. They have insight into population flow and have learned to incorporate their collective knowledge and work together to arrive at the most efficacious and humane policy decisions. Their input would be invaluable in any policy decision-making that involved federal officials.

15.3.1.7 **Congress should provide funding to leverage and support existing national public service advertising campaigns to educate the U.S. public and migration source countries about illegal migration and the humanitarian toll of failing to secure the border.**

This education campaign would serve as an informational deterrent to those who may desire to enter this country illegally and better inform the public about the humanitarian crisis on the Southwest Border. Both those planning to come illegally and those who are already American citizens may be unaware of the potential for criminal, financial, and sexual victimization or death due to environmental hazards. Additionally, such a campaign would generate wider support for border security efforts by providing clear information about how the lack of border security incentivizes and encourages the dangerous activity of illegal

[67] Leon Wilmot, Sheriff, Yuma County Sheriff's Office, Homeland Security Working Group Member, in discussion with the Homeland Security Working Group, Border Security Meeting, April 20, 2020.
[68] State Criminal Alien Assistance Program Overview, www.bja.ojp.gov
[69] Mark Dannels, Sheriff, Cochise County Sheriff's Office; Mark Napier, Sheriff, Pima County Sheriff's Department; and Leon Wilmot, Sheriff, Yuma County Sheriff's Office, Homeland Security Working Group Member, in discussion with the Homeland Security Working Group, Border Security Meeting, April 20, 2020.

immigration.

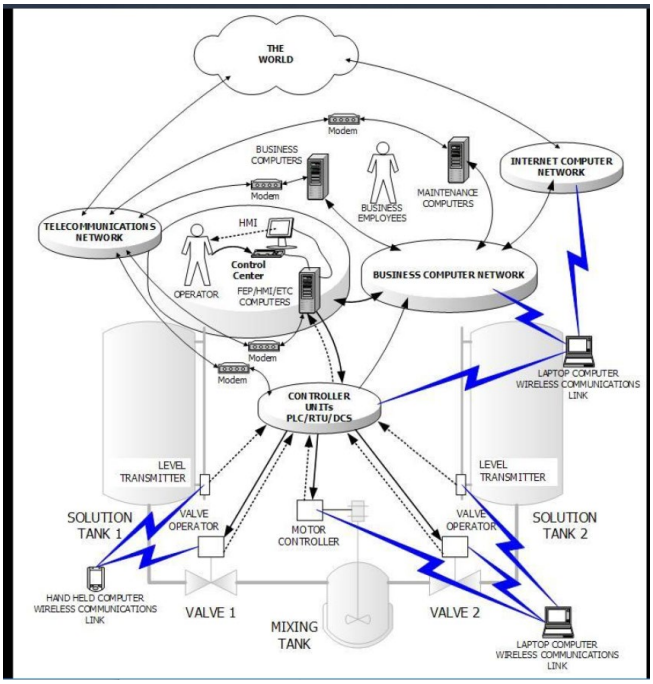
This crisis, focusing in particular on human smuggling, was highlighted by Sergeant Joshua Coleman, Texas Department of Public Safety: "The criminal organizations . . . do not care about the socio-economic situation of the persons they are trying to recruit or kidnap. It's about making money and turning a profit no matter what lives these individuals destroy." He added that educating the public "to show the adverse effects of human trafficking and its illicit behavior can rally our communities [who can then] assist in countering this deviant behavior."[70]

Cybersecurity and Soft Targets 15.3.2

15.3.2.1 **Congress should provide additional funding to enhance the Federal Bureau of Investigation's efforts to educate state, local, territorial, and tribal organizations and non-governmental entities about the need to harden their cyber infrastructure.**

Because of funding limitations, many government agencies and other critical infrastructures operate with end-of-life, obsolete, or outdated technology, which makes them vulnerable to cyberattack. Entities that consider themselves low risk or that struggle to attract and retain talented technological staff may also delay implementing critical updates, patches, or other protective measures. Comprehensive efforts to plan for and replace systems before they reach end of life, upgrade outdated technology, train and retain skilled staff, and provide clear implementation requirements of critical updates that can be routinely audited are necessary to ensure entities can protect against and mitigate attacks from cyber threat actors.[71]

Understanding Control System Cyber Vulnerabilities



Source: U.S. Computer Emergency Readiness Team (U.S.CERT); To understand the vulnerabilities associated

[70] Joshua Coleman, Sergeant, Texas Department of Public Safety, Public Comment to the President's Commission on Law Enforcement and the Administration of Justice, submitted April 22, 2020.
[71] Richard L. Swearingen, Commissioner, Florida Department of Law Enforcement (FDLE) and Special Agent in Charge Shane Desguin (FDLE) Public Comment to the President's Commission on Law Enforcement and the Administration of Justice, April 30, 2020.

with control systems (CS), you must first know all of the possible communications paths into and out of the CS. This figure presents various devices, communications paths, and methods that can be used for communicating with typical process system components. [72]

15.3.2.2 **The Federal Bureau of Investigation and Department of Homeland Security's Cybersecurity and Infrastructure Agency should provide additional briefings and information to state, local, tribal, and territorial government technological procurement offices regarding companies and components known to carry cybersecurity risks**.

Some adversaries likely engage in cyber espionage, which includes obtaining cyber information accessible to companies that are operating in their country. It can be difficult for state, local, trial, and territorial governments to identify companies or technology with ties to these countries due to the number of subsidiaries, lack of visibility on components and their manufacturers, and the tendency for many commercial off-the-shelf products to arrive pre-loaded with software. Resources or guidance for procurement officers on how to identify potential vulnerabilities can enable state, local, trial, and territorial governments to make better technological purchasing decisions, which will protect the nation's cyber infrastructure. [73]

15.3.2.3 **The Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, in coordination with federal departments and agencies, should develop a comprehensive resource guide for state, local, tribal, and territorial law enforcement that contains information about the federal government capabilities that are readily available to support strengthening soft targets and crowded places, such as sports stadiums and arenas, performing arts centers, and outdoor gathering places.**

There are many resources available to state, local, tribal, and territorial law enforcement and venue operators to help them better fortify soft targets and crowded places. The federal government should compile all of its resources in a user-friendly guide that includes information about conducting risk and vulnerability assessments. In addition, this guide should list which FEMA grants are available to local and state governments to support soft target preparedness activities through the State Homeland Security Program (SHSP) and the (UASI). The recent DHS Notice of Funding Opportunities, which prioritizes enhancing the protection of soft targets and crowded places (including election security), will encourage state and local jurisdictions to leverage their grant dollars to strengthen large venues and other soft targets. By so doing, these jurisdictions will better protect the public from potential threats.[74]

The resource guide should also include information about DHS's Support Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act authority. This act was designed to provide liability protection in the event a plaintiff claimed a product or service (including cyber-related) did not provide sufficient protection from an act of terrorism.

Appendix A: Methodology

Virtual Site Visit

On April 16, the Homeland Security Working Group participated in a virtual field visit to the Orange County Intelligence Assessment Center (OCIAC) in California. The OCIAC is one of the 80 fusion centers that comprise

[72] https://www.us-cert.gov/sites/default/files/transimages/figure1.jpg
[73] Richard L. Swearingen, Commissioner, Florida Department of Law Enforcement (FDLE) and Special Agent in Charge Shane Desguin (FDLE) Public Comment to the President's Commission on Law Enforcement and the Administration of Justice, April 30, 2020.
[74] The Department of Homeland Security (DHS) Notice of Funding Opportunity (NOFO) Fiscal Year (FY) 2020 Homeland Security Grant Program (HSGP), p. 3. https://www.fema.gov/media-library/assets/documents/185911 accessed May 7, 2020.

the National Network of Fusion Centers. The OCIAC staff and partners provided an overview of its role and functions and explained how the OCIAC collaborates with other agencies and other fusion centers. The agenda topics included presentations from the outreach unit; partner engagement unit; critical Infrastructure unit: Providing Vulnerability Assessments; Analysis: Partnerships and Target Discovery; Tips and Leads; and Perspective from the FBI and DHS partners.

Orange County Intelligence Assessment Center (April 16, 2020)

- Alberto Martinez, Deputy Director, Orange County Sheriff's Department / OCIAC
- Chris Hays, Director, Orange County Sheriff's Department / OCIAC
- Nick Freeman, Fire Captain, Orange County Fire Authority / OCIAC
- Greg Fox, Fire Captain, Anaheim Fire and Rescue / OCIAC
- Jonathan Hill, OCIAC
- Manny Cruz, Sergeant, Orange County Sheriff's Department / OCIAC
- Linda Pototsky, Intelligence Analyst, Los Angeles Field Office, FBI
- Krystal Lugaila, Acting Senior Supervisory Intelligence Analyst, Los Angeles Field Office, FBI
- Anthony Frangipane, Jr., Southwest Regional Director, Field Operations, Office of Intelligence & Analysis, DHS
- Joshua Stone, Acting Special Agent in Charge, National Security Division, Lost Angeles Field Office, FBI
- Roland Andrade, Sergeant, Santa Ana Police Department, Urban Area Grants Coordinator

Literature search

Received annotated bibliographies on the following topics

- Blind Spots
- Border Security
- Domestic Terrorism
- Fusion Centers
- Government Resources
- Information-Sharing
- International Terrorism
- Lone Actors
- Partnerships
- Radicalization
- Soft Targets

Subject Matter Expert Briefings

Identifying the Nature of the Threat - April 6, 2020

(Domestic Terrorism; International Terrorism)

Presenters:

- Debra Anderson, Unit Chief, Domestic Terrorism Analysis Unit, Federal Bureau of Investigation
- Dr. Robert Friedmann, Founding Director, Georgia International Law Enforcement Exchange, Georgia State University
- Seamus Hughes, Deputy Director, Program on Extremism, George Washington University
- Timothy Gruber, Chief for Protective Intelligence, U.S. Marshals Service

Partnerships and Information-Sharing - April 13, 2020

Presenters:

- Colonel Mark Poland, Undersheriff, Loudoun County Sheriff's Office
- Russ Porter, Chief of Strategic Partnerships, National Counterintelligence and Security Center, Office of the Director of National Intelligence
- Alberto Martinez, Deputy Director, Orange County Intelligence Assessment Center
- David Ring, Assistant Section Chief, Counterterrorism Division, FBI
- Sarah Chervenak, Unit Chief, Office of Partner Engagement, FBI
- Ray Guidetti, Lieutenant Colonel Ray Guidetti (NJSP ret.), Industry Specialist Intelligence-led Public Safety Software Enterprise, Motorola Solutions (retired Lieutenant Colonel, New Jersey State Police)

Border Security and Transnational Organized Crime – April 20, 2020

Presenters:

- Sheriff Mark Dannels, Cochise County (AZ) Sheriff's Office
- Director Steven McCraw, Texas Department of Public Safety
- Section Chief Michael Nordwall, Transnational Organized Crime Global, FBI
- Executive Director Roland Suliveras, National Targeting Center-Cargo, U.S. Customs and Border Protection
- Sheriff Mark Napier, Pima County, Arizona Sheriff's Department

Vulnerabilities/Threats - April 27, 2020

Presenters:

- Jeff Miller, Vice President of Security, Kansas City Chiefs
- Brian Murphy, Principal Deputy Undersecretary, DHS Office of Intelligence and Analysis
- Kevin Peters, Chief, National Threat Evaluation and Reporting Program, DHS Office of Intelligence
- and Analysis
- John Miller, Deputy Commissioner, Intelligence and Counterterrorism, New York City Police Department
- Thomas Galati, Chief, Intelligence Bureau, New York City Police Department

Target Identification and International Operations - May 4, 2020

Presenters:

- Paul Knierim, Chief of Intelligence, Drug Enforcement Administration
- Tom Sobocinski, Deputy Assistant Director, International Operations Division, Federal Bureau of Investigation

Lawful Access (hosted by the Technology Working Group) – May 15, 2020
Moderator:

- Darrin E. Jones, Executive Assistant Director, Science and Technology Branch, Federal Bureau of Investigation

Presenters:

- Stewart Baker, host of The Cyberlaw Podcast
- Elizabeth Banker, Deputy General Counsel, Internet Association

Data

Business Meetings (conference calls)

- March 9 – Kick-Off Call
- March 23 – Implementation Call
- April 16 – Annotated Outline, Recommendations, and Timeline
- April 24 – Identifying the Nature of the Threat Recommendations Discussion
- April 30 – Information-Sharing and Partnership Recommendations Discussion
- May 5 – Border Security Recommendations Discussion
- May 7 – Vulnerability Recommendations Discussion and discussion of revised and new recommendations
- May 27, 2020 – Homeland Security Draft Chapter Discussion
- June 1, 2020 – Homeland Security Working Group Meeting/Updates
- June 15, 2020 – Homeland Security Working Group Meeting/Updates

Technical Calls (conference calls)

- April 17 – ODNI (Russ Porter)
- May 1 – FBI and ODNI (Sarah Chervenak and Russ Porter)
- May 1 and May 4 - DHS I&A State and Local Partner Engagement – Alethea Madello and Susan Bower
- May 8 – National Fusion Center Association (Ben Bawden, Mike Sena, Alberto Gonzalez, Chris Hays, and Chris DeRemer; and Sheriff Mike Chapman, Homeland Security Working Group Co-Chair)
- May 11 – FEMA and CBP - Operation Stonegarden (Mark Silveira, Maurice (Mo) Gill, Michael Hammert, and Dustin Judd)
- May 13 – U.S. Probation and Parole (Paul Brennan, Jay Whetzel, and Trent Cornis; and U.S. Attorney Richard Donoghue, Homeland Security Working Group Member)
- May 14 – DHS Cybersecurity and Infrastructure Security Agency (Daniel Abreu)