## 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]

### Overview

It was not until the terrorist attacks of September 11, 2001 that the term "homeland security" entered the national lexicon. Since then, the threats to the general security of the American people have expanded and diversified. Today, these threats come in many different forms, including foreign terrorist organizations (FTOs), radicalized lone actors, domestic violent extremists, foreign malign influence campaigns by nation-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 intelligence agencies needed to improve their ability to "connect the dots."[2] In the aftermath of 9/11, government agencies have made significant progress in instituting protocols to share rather than shield information, and information that was once compartmentalized is now collected and available across the intelligence community (IC) as well as federal, state, local, and tribal 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 into a unified, integrated cabinet agency.[3]

In examining the role of law enforcement in promoting homeland security and preventing attacks against the United States, the Commission has determined that while post-9/11 informational capabilities of law enforcement and the intelligence community has progressed substantially, there are still areas for further improvement in the development, gathering, and access of law enforcement agencies to homeland security information—particularly in the context of federal partnerships with state, local, and tribal law enforcement agencies in combatting homegrown violent extremism and domestic terrorism. Moreover, the Commission has also assessed the need for greater awareness, coordination, and resources to address homeland security risks posed by territorial borders and cyberspace.

The federal government made other significant changes to address homeland security after 9/11. The Federal Bureau of Investigation (FBI) shifted its priorities to counterterrorism, counterintelligence, and cyber security.[4] The Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458; 118 Stat. 3688 (2004), 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 after 9/11. The ODNI's mission is to lead and support IC integration, deliver insights, drive capabilities, and invest in the future. Notably, the biggest change in

---

[1] Bridget Johnson, "Wray: Racial Violent Extremism Is a Top Priority for FBI 'on the Same Footing as ISIS,'" Homeland Security Today, February 6, 2020, https://www.hstoday.us/subject-matter-areas/counterterrorism/wray-racial-violent-extremism-is-a-top-priority-for-fbi-on-the-same-footing-as-isis/.

[2] National Commission on Terrorist Attacks Upon the United States, *Final Report of the National Commission on Terrorist Attacks Upon the United States* (New York: Norton, 2004), 408, https://www.9-11commission.gov/report/.[3] "About DHS," U.S. Department of Homeland Security, accessed June 22, 2020, https://www.dhs.gov/about-dhs.

[3] "About DHS," U.S. Department of Homeland Security, accessed June 22, 2020, https://www.dhs.gov/about-dhs.

[4] *U.S. House Appropriations Subcommittee on Commerce Justice, Science, and Related Agencies: Transformation of the Federal Bureau of Investigation* (September 14, 2006) (statement of Robert S. Mueller, III, Director, Federal Bureau of Investigation), https://archives.fbi.gov/archives/news/testimony/the-fbi-transformation-since-2001.[5] Matthew Alcoke, Deputy Assistant Director, Federal Bureau of Investigation, "The Evolving and Persistent Terrorism Threat to the Homeland," presented at Washington Institute for Near East Policy Counterterrorism Lecture Series, Washington, DC, November 19, 2019.

American law enforcement over the past 50 years has been recognizing the importance of collaborating across all levels of government and with the communities they serve.

In its deliberations, 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, and tribal entities; and protect the homeland for future generations.

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

Nearly 20 years have passed since al-Qa'ida (AQ) attacked the United States. Terrorist organizations across the globe like AQ and the Islamic State of Iraq and ash-Sham (ISIS) continue to harbor the intent 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 who are often the first to raise the alarm when observing suspicious activity in their jurisdiction

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 who have been inspired by foreign terrorist organizations have 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 domestic violent extremists (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 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.[5] While ISIS continues to be a key influence, it is one of several violent extremist influences that contribute to subjects' radicalization and mobilization. For example, now-deceased ideologue and al-Qa'ida in the Arabian Peninsula senior leader Anwar al-Awlaki, a Yemeni-American jihadist, remains a key influence more than nine years after his death.[6] Since 2014, there have been more than 200 people in the United States charged with offenses related to ISIS.[7]

Like HVEs, DVEs continue to be inspired by a mix of ideological, sociopolitical, and personal factors that vary widely based on individual circumstances. The FBI categorizes DVEs as racially or ethnically motivated violent extremists (RMVE), anti-government/anti-authority extremists, abortion-related extremists, or animal rights/environmental extremists.[8] Drivers for most DVEs include perceptions of government or law enforcement overreach, sociopolitical conditions, and reactions to legislation or national events. These trends are primarily enabled by the internet and social media, which facilitates DVEs engaging with others

[5] Matthew Alcoke, Deputy Assistant Director, Federal Bureau of Investigation, "The Evolving and Persistent Terrorism Threat to the Homeland," presented at Washington Institute for Near East Policy Counterterrorism Lecture Series, Washington, DC, November 19, 2019.
[6] Scott Shane, "The Enduring Influence of Anwar al-Awlaki in the Age of the Islamic State," *CTC Sentinel* 9, no. 7 (2016), https://www.ctc.usma.edu/the-enduring-influence-of-anwar-al-awlaki-in-the-age-of-the-islamic-state/.
[7] Seamus Hughes, Deputy Director, Program on Extremism, George Washington University, in discussion with Homeland Security Working Group, virtual meeting, April 6, 2020.
[8] (U//LES) Federal Bureau Investigation, "Counterterrorism 2020: Domestic Terrorism Threat Overview" (PowerPoint presentation, Washington, DC, April 2020).

without having to join organized groups. This online communication enables the sharing of literature promoting DVE beliefs, including 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.[9] In 2019, DVE attacks in the United States resulted in the death of 32 individuals, making 2019 the deadliest year in domestic terrorism since the 1995 bombing of the federal building in Oklahoma City that killed 168 individuals.[10]

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 are often the first responders, as seen in 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."[11] They published *Promising Practices for Using Community Policing to Prevent Violent Extremism* offering recommendations for a whole-of-government approach that includes planning, training, and community outreach and engagement.[12]

In recent years, lethal domestic terrorist attacks have been primarily perpetrated by lone DVEs or by 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 shared across online platforms by DVEs. DVEs also use these platforms to promote potentially radicalizing hate speech and post manifestos outlining grievances. Racial or ethnic minority groups, religious groups, law enforcement, and government personnel and facilities are often the primary targets. The law enforcement community continues to be challenged by the individualized nature of the radicalization and mobilization processes and the difficulty of distinguishing between violent rhetoric and actual terrorist intent.

As the threats to the United States continue to evolve, advances in technology have made it easier for adversaries to communicate and share information via social media and mobile devices.[13] Unfortunately, law enforcement is hindered in its ability to leverage those tools for investigative purposes.[14]

Many of these recommendations transcend both international and domestic terrorism threats.

### 15.1.1 Congress should enact legislation that guarantees law enforcement agencies equal and lawful access to publicly posted data.

Over the past few years, social media companies have added language to their terms of service that prohibits law enforcement from using Application Programming Interfaces (API) 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 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, such as 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 that have traditionally been made by elected officials are now being

---

[9] (U//LES) Federal Bureau Investigation, "Counterterrorism 2020."[10] Anderson, in discussion with Homeland Security, April 6, 2020.
[10] Anderson, in discussion with Homeland Security, April 6, 2020.
[11] Elizabeth Miller, Jessica Toliver, and David Schanzer, *Promising Practices for Using Community Policing to Prevent Violent Extremism: How to Create and Implement an Outreach Plan* (Washington, DC: Police Executive Research Forum, 2016), 3, https://www.policeforum.org/assets/usingcommunitypolicingtopreventviolentextremism.pdf.
[12] Miller, Toliver, and Schanzer, *Promising Practices*.[13] Debra Anderson, Unit Chief, Domestic Terrorism Analysis Unit, Federal Bureau of Investigation, and Seamus Hughes, Deputy Director, Program on Extremism, George Washington University, in discussion with Homeland Security Working Group, virtual meeting, April 6, 2020.
[13] Debra Anderson, Unit Chief, Domestic Terrorism Analysis Unit, Federal Bureau of Investigation, and Seamus Hughes, Deputy Director, Program on Extremism, George Washington University, in discussion with Homeland Security Working Group, virtual meeting, April 6, 2020.
[14] David Bowdich, Deputy Director, Federal Bureau of Investigation, in discussion with Homeland Security Working Group, virtual meeting, May 7, 2020.

made by corporate chiefs. Law enforcement operating under the rule of law and abiding by the proper constraints and authorizations set forth by the Constitution and congressional action should have access to this data

The proposed legislation would prevent social media companies from excluding government agencies or their agents from assembling, reviewing, and exploiting publicly posted data if they allow other entities (e.g., marketers) to access and analyze the data. 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 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 notifying the local Joint Terrorism Task Force and governors so they can alert their respective criminal justice authorities.

Local, state, tribal, and federal law enforcement officials should 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.[15] 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.[16]

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 both inmates charged with federal or state non-terrorism crimes who have a connection to international or domestic terrorism and inmates charged with federal terrorism charges. State and local authorities should notify the local Joint Terrorism Task Force (JTTF) and governors when offenders 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.

### 15.1.6 State, local, and tribal law enforcement should voluntarily 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, and tribal law enforcement, the collection of domestic terrorism incidents should be added to information received from the more than 18,000 law enforcement agencies who voluntarily participate in the FBI's Uniform Crime Report (UCR) program. The data should be submitted through a state UCR program or directly to the federal UCR program, and it should be included in the National Incident-Based Reporting System beginning in 2021.

**[CROSS REFERENCE DATA AND REPORTING]**

---

[15] (U//FOUO) Federal Bureau of Investigation, *Identifying and Mitigating Extremist Activities in Corrections* (Washington, DC: Federal Bureau of Investigation, 2020), 1.

[16] Richard Donoghue, U.S. Attorney, Eastern District of NY, email communication with Amy Schapiro, Federal Program Manager, Homeland Security Working Group, June 11, 2020.[17] "National Network of Fusion Centers Fact Sheet," U.S. Department of Homeland Security, accessed June 23, 2020, https://www.dhs.gov/national-network-fusion-centers-fact-sheet; Rachel A. Seitz, Enterprise Performance and Evaluation, U.S. Department of Homeland Security, email communication with Amy Schapiro, Federal Program Manager, Homeland Security Working Group, May 8, 2020; and Alberto Martinez, Deputy Director, Orange County Intelligence Assessment Center, CA, in discussion with Homeland Security Working Group, virtual meeting, April 13, 2020.

### 15.2 Information-Sharing and Partnerships

As noted above, in the aftermath of the September 11th attacks law enforcement agencies have recognized the importance of a collaborative framework for gathering and sharing information. 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, and tribal communities, and vice versa. The National Network of Fusion Centers (the Network) comprises 80 fusion centers across all states and territories that are staffed and operated by state and local governments, with support from federal partners.[17] They facilitate two-way intelligence and information flow among the federal government; state, local, and tribal agencies; and private sector partners. Fusion centers conduct analysis and facilitate information sharing. In doing so, they help law enforcement, fire, public health, homeland security, emergency management, and private sector critical infrastructure partners prevent, protect against, and respond to crime and terrorism. The Network plays a critical role in enhancing the nation's ability to support public safety and counterterrorism missions. They also assist in federal investigations.

Many private sector entities have partnered with federal agencies to share critical data related to travel and global supply chains.[18] DHS established the Public-Private Analytic Exchange Program, which 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 success. Participants work to create unclassified joint analytic deliverables of interest to both the private sector and the federal government.

[17] "National Network of Fusion Centers Fact Sheet," U.S. Department of Homeland Security, accessed June 23, 2020, https://www.dhs.gov/national-network-fusion-centers-fact-sheet; Rachel A. Seitz, Enterprise Performance and Evaluation, U.S. Department of Homeland Security, email communication with Amy Schapiro, Federal Program Manager, Homeland Security Working Group, May 8, 2020; and Alberto Martinez, Deputy Director, Orange County Intelligence Assessment Center, CA, in discussion with Homeland Security Working Group, virtual meeting, April 13, 2020.

[18] Roland Suliveras, Executive Director, National Targeting Center-Cargo, U.S. Customs and Border Protection, in discussion with Homeland Security Working Group, virtual meeting, April 27, 2020.


Source: Department of Homeland Security, Office of Intelligence and Analysis, Office of State and Local Partner Engagement

Law enforcement agencies at all levels of government have established strong 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.

### 15.2.1 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 the National Network of Fusion Centers.

Anecdotal evidence shows that fusion centers benefit from federal personnel being co-located at a fusion center. According to the DHS' 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.[19] However, the number of personnel is considerably smaller 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 nine employees in fusion centers. The DEA, the Transportation Security Agency, U.S. Customs and Border Protection (CBP), and the Federal Law Enforcement Training Center all have either one or two representatives.[20]

Without specific appropriated funding, federal law enforcement agencies have not been able to dedicate the needed personnel to enhance fusion centers risking a return to the pre-9/11 intelligence failures

[19] Seitz, email communication to Amy Schapiro, May 8, 2020.
[20] Seitz, email communication to Amy Schapiro, May 8, 2020. Data for personnel assigned from federal agencies are derived from a U.S. Department of Homeland Security Office of Intelligence and Analysis Federal Cost Inventory (annual data call). Data received are based on whether they receive responses from those components or agencies. These data are based on responses to the 2018 Federal Cost Inventory.

**15.2.2 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 comprising the National Network of Fusion Centers.**

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 intended for 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 can plan, build, and maintain capabilities that are essential to their missions.

**15.2.3 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 training proposed by this commission ensures that local leaders are briefed and understand the criminal and intelligence threat pictures. By providing a fuller understanding of the information and intelligence landscape through training, state and local authorities will be 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.

**15.2.5 The Department of Homeland Security should survey state, local, and tribal law 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.**

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. Special focus should be placed on information systems that can inform behavioral threat assessment processes and assist in the threat management process. 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[21]

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 context. He views border security as needing a three-tiered approach, addressing public safety, national security, and human rights.[22] Robust border security gives law enforcement and national security officials the capability to evaluate, identify, and prevent incursions by foreign terrorist actors who seek to enter the United States with designs to injure the country. And while acknowledging the vast majority of attention is focused on national security, drug smuggling, gangs, sex trafficking, human smuggling, and illegal aliens, border security must be addressed as a humanitarian issue as well.

[21] Mark Napier, Sheriff, Pima County Sheriff's Department, AZ, in discussion with Homeland Security Working Group, virtual meeting, April 20, 2020.
[22] Napier, in discussion with Homeland Security, April 20, 2020.

In addition to efforts to secure the Southwest Border, another area of concern is the safety and security of the public while attending large and crowded gathering places, such as sports venues, nightclubs, concerts, and movies. Attacks on such places have occurred 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.

Such locations are grouped under the term "soft targets" and crowded places-- 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.[23]

In a conversation with the Homeland Security Working Group, Jeff Miller, vice president of security for the Kansas City Chiefs football team, discussed the multiple risks seen at such venues, ranging from active shooters to critical infrastructure failures. Once these vulnerabilities and their potential consequences are brought to the attention of decision-makers who preside over large venues, they often dedicate the needed funds for hardening their premises.[24] While Mr. Miller spoke in detail about safely securing sports stadiums, he along with Chief Thomas Galati, New York City Police Department (NYPD), 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.[25]

**[BEGIN TEXT BOX**]

The Homeland Security Grant Program, administered by FEMA, makes funds available to local and state governments to support soft target preparedness activities. Further information is available at: https://www.fema.gov/homeland-security-grant-program.

In addition to funding, DHS has several publications available, including a guidebook 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. A number of fact sheets are also available.

The following publications related to securing large events are available from the Department of Justice Office of Community Oriented Policing Services and the Bureau of Justice Assistance:

*Planning and Managing Security for Major Special Events: Guidelines for Law Enforcement*:

https://cops.usdoj.gov/RIC/Publications/cops-w0703-pub.pdf

*Planning and Managing Security for Major Special Events: Training Curricula:*

https://cops.usdoj.gov/RIC/ric.php?page=detail&id=COPS-CD026

*Managing Large-Scale Security Events: A planning Primer for Law Enforcement Agencies:*

https://bja.ojp.gov/sites/g/files/xyckuh186/files/Publications/LSSE-planning-Primer.pdf

**[END TEXT BOX]**

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

---

[23] U.S. Department of Homeland Security, *Notice of Funding Opportunity Fiscal Year 2020 Homeland Security Grant Program* (Washington, DC: U.S. Department of Homeland Security, 2020), 3, https://www.fema.gov/media-library-data/1583442273016-07cbcf9445f9fda3cdc5bf8439ec72c9/FY_2020_HSGP_NOFO_FINAL_508ML4.pdf.

[24] Jeff Miller, Vice-President of Security, Kansas City Chiefs, in discussion with Homeland Security Working Group, virtual meeting, April 27, 2020.

[25] Jeff Miller, Vice President of Security, Kansas City Chiefs, and Thomas Galati, Chief Intelligence Bureau, New York City Police Department, in discussion with the Homeland Security Working Group, virtual meeting, April 27, 2020.

> Virtually every national security threat and crime problem the FBI faces is cyber-based or -facilitated. We face threats from state-sponsored hackers, hackers for hire, organized cyber syndicates, and terrorists. On a daily basis, these actors seek to steal our state secrets, our trade secrets, our technology, and the most intimate data about our citizens—things of incredible value to all of us and of great importance to the conduct of our government business and our national security. They seek to hold our critical infrastructure at risk, to harm our economy, and to constrain our free speech.[26]

Border Security

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

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.

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 should provide adequate controls to manage and mitigate illegal migration flows, which should therefore improve national security and the safety of the American people.

**15.3.2 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 without any aggravating factors 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.

**15.3.3 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 Immigration and Customs Enforcement (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 deported according to established immigration laws and procedures.

**15.3.4 Congress should enact legislation that provides an authorization and an increased appropriation for the Department of Homeland Security's Operation Stonegarden grant program, which provides funding for border operations and other resources geared for law enforcement agencies along the national border.**

**[CROSS-REFERENCE GRANTS]**

[26] Wray, *U.S. House Judiciary Committee*, February 5, 2020, 5.

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 OPSG would enable a whole-of-community, counter-network approach to defeat transnational criminal organizations and provide front-line anti-terrorism defense of the nation.

**15.3.5 Congress should authorize and appropriate funds to the Department of Justice to establish a grant 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 jurisdictions. 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 who have been 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.[27] 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 or two misdemeanor convictions for violations of state or local law and who are incarcerated for at least four consecutive days during the reporting period.[28] Yet, border sheriffs say this is not enough because the aid provided is equivalent to roughly five cents on the dollar for their expenditures, which does not begin to cover their incurred expenses.[29]

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. It will also provide needed funds to address the mounting humanitarian, public safety, and national security issues that law enforcement on the Southwest border encounter daily.

The need for grant funding was highlighted during a series of roundtables and focus groups that the National Sheriffs Association and the COPS Office hosted with border sheriffs. They found that

> sheriffs need funding to secure full-time personnel, both commissioned and support staff. Many grants such as the DHS's Operation Stonegarden only provide resources for equipment or overtime funds—which are important, but without the personnel to use those resources, the net benefit of that funding becomes moot. Increased personnel must include not only permanent deputies but also the support staff to alleviate their workload by helping in activities such as operation coordination and maintaining grant funding. In addition, northern border sheriffs need increased personnel to patrol the larger counties.[30]

In addition, "border sheriffs also require more resources in the form of improved equipment, technology, and vehicles to better patrol remote border areas, assist in opening lines of communication in dead zones, improve surveillance along the border, and equip officers with the things they need to more effectively do

---

[27] Leon Wilmot, Yuma County Sheriff's Office, AZ, in discussion with Homeland Security Working Group, virtual meeting, April 20, 2020.
[28] "State Criminal Alien Assistance Program Overview," Bureau of Justice Assistance, accessed June 24, 2020, https://bja.ojp.gov/program/state-criminal-alien-assistance-program-scaap/overview.
[29] Mark Dannels, Sheriff, Cochise County Sheriff's Office, AZ, Mark Napier, Pima County Sheriff's Department, AZ, and Leon Wilmot, Yuma County Sheriff's Office, AZ, in discussion with Homeland Security Working Group, virtual meeting, April 20, 2020.[30] Barksdale and Yount, *Unique Needs and Challenges of Border*, 4.
[30] Barksdale and Yount, *Unique Needs and Challenges of Border*, 4.

their jobs. Along the northern border, equipment is needed to patrol inaccessible areas such as waterways or snow embankments: boats, snowmobiles, ATVs, improved cameras, and updated radio systems that switch to 800 MHz."[31] It is because of this vast need that a new grant program is needed for law enforcement border agencies.

### 15.3.6 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 and Northern 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 to arrive at the most efficacious and humane policy decisions. Their input would be invaluable in any policy decision making that involves federal officials.

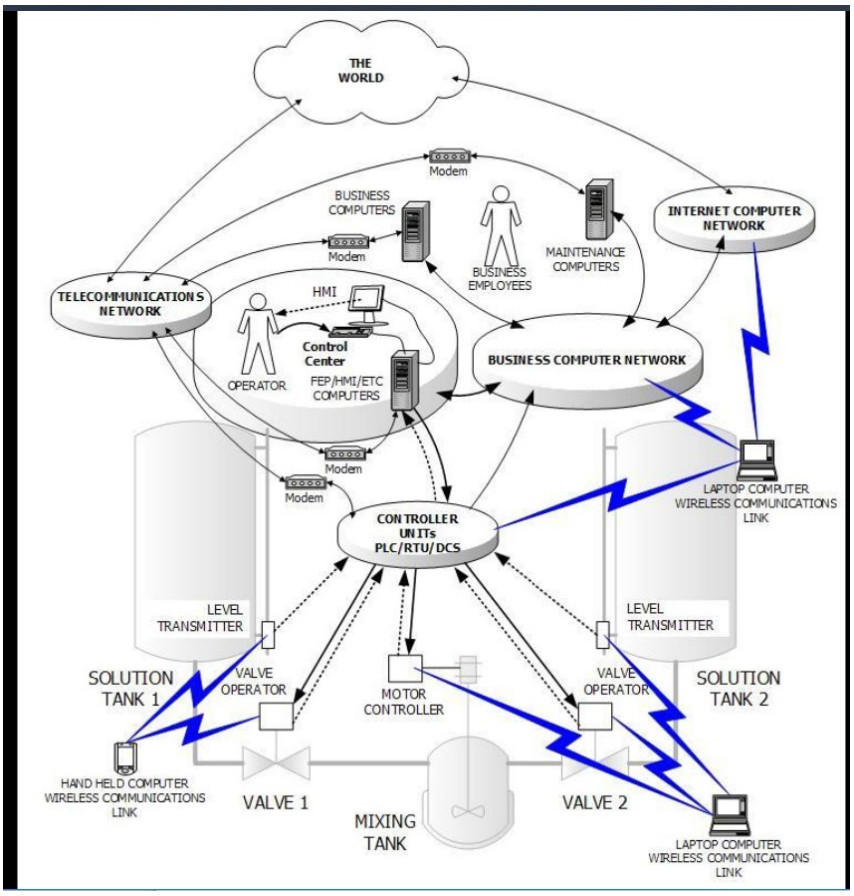
Border sheriffs have advocated for a better system to coordinate with federal partners, and for an effective, balanced voice for border law enforcement at the table of policy discussion. Sheriffs have also expressed their frustration with the lack of coordination between state immigration laws and federal enforcement guidelines, which in many cases are in direct conflict. Furthermore, policymakers setting those laws and guidelines have focused heavily on the southern border, neglecting issues facing northern border law enforcement.[32] With border sheriffs at the table, policies can be more effectively developed and implemented.

[31] Barksdale and Yount, *Unique Needs and Challenges of Border*, 4.

[32] Barksdale and Yount, *Unique Needs and Challenges of Border*.[33] Richard L. Swearingen, Commissioner, and Shane Desguin, Special Agent in Charge, Florida Department of Law Enforcement, public comment to President's Commission on Law Enforcement and the Administration of Justice, April 30, 2020.

Cybersecurity and Soft Targets

**Understanding Control System Cyber Vulnerabilities**




Source: U.S. Computer Emergency Readiness Team

### 15.3.7 The Federal Bureau of Investigation and Department of Homeland Security's Cybersecurity and Infrastructure Agency should inform state, local, and tribal government technological procurement offices regarding companies and components known to carry cybersecurity risks.

Foreign adversaries may 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, and tribal governments to identify companies or technology with ties to these countries due to the number of subsidiaries; the 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, and tribal governments to make better technological purchasing decisions, which will protect the nation's cyber infrastructure.[33]

[33] Richard L. Swearingen, Commissioner, and Shane Desguin, Special Agent in Charge, Florida Department of Law Enforcement, public comment to President's Commission on Law Enforcement and the Administration of Justice, April 30, 2020.